

# Physical characteristics of wireless communication channels for secret key establishment: A survey of the research

## Journal Item




# Physical Characteristics of Wireless Communication Channels for Secret Key Establishment: A Survey of the Research

Mirko Bottarelli, Gregory Epiphaniou, Dhouha Kbaier Ben Ismail, Petros Karadimas, Haider Al-Khateeb

PII: S0167-4048(18)30084-1
DOI: https://doi.org/10.1016/j.cose.2018.08.001
Reference: COSE 1377

To appear in: *Computers & Security*

Received date: 14 February 2018
Revised date: 31 July 2018
Accepted date: 1 August 2018

Please cite this article as: Mirko Bottarelli, Gregory Epiphaniou, Dhouha Kbaier Ben Ismail, Petros Karadimas, Haider Al-Khateeb, Physical Characteristics of Wireless Communication Channels for Secret Key Establishment: A Survey of the Research, *Computers & Security* (2018), doi: https://doi.org/10.1016/j.cose.2018.08.001

# Physical Characteristics of Wireless Communication Channels for Secret Key Establishment: A Survey of the Research

Mirko Bottarelli[a], Gregory Epiphaniou[a], Dhouha Kbaier Ben Ismail[a], Petros Karadimas[b], Haider Al-Khateeb[a]

[a] *Wolverhampton Cyber Research Institute (WCRI), School of Mathematics and Computer Science, University of Wolverhampton, Wulfruna Street, Wolverhampton, UK*
[b] *University of Glasgow, School of Engineering, Glasgow, Scotland*

**Abstract**

Physical layer security protocols have recently been deployed in the context of Wireless communications. These are derived from the intrinsic characteristics of the communication media for key generation, sharing and randomness extraction. These protocols always seek to exhibit both low computational complexity and energy efficiency, whilst also maintain unconditionally secure communications. We present herein, a comprehensive literature review of existing "state-of-the-art" quantisation schemes for physical layer security, with a strong emphasis upon key performance metrics and intrinsic channel characteristics. Our survey seeks not only to concentrate upon the most common quantisation methods, hence their efficiency during key generation; but also crucially, describes the inherent trade-offs as between these standardised metrics. The exact way(s) in which these metrics are duly influenced by quantisation schemes is also discussed, by means of a comprehensive critical narrative of both existing and future developments in the field.

*Keywords:* key generation, physical layer security, quantisation, wireless channels

## 1. Introduction

The exponential growth of wireless communication systems, such as wireless sensor networks (WSNs) and vehicle ad-hoc networks (VANETs), draws an increasing interest with regards to privacy and security due to the broadcasting nature of the wireless communication channel. This security problem consists in the transmitter Alice which sends private messages to the legitimate

*Corresponding author
*Email address:* g.epiphaniou@wlv.ac.uk (Gregory Epiphaniou)

receiver Bob through an insecure channel, in the presence of a passive eavesdropper Eve, whose aim is to extract the original payload using her observations.

Securing a communication means putting the adversary in a disadvantageous position with respect to the legitimate receiver. Such a situation is commonly obtained by the adoption of traditional cryptographic techniques to encode/decode communication content [1]. In these protocols, security is considered as an independent feature to the channel properties, built on the assumption that an error-free physical layer has already been established.

In public key cryptography, a centralised trusted authority generates, distributes and maintains key-pairs to communicators, which implies a high key-management complexity and intensive key distribution to support the key establishment [2, 3]. This kind of approaches rely on computational complexity, however are not suitable for low-end wireless devices, as demonstrated in Diffie-Hellman [4] and RSA algorithms. On the other hand, symmetric cryptography has the potential of achieving high security and low overhead, but its application scenarios are severely reduced by the complex task of generating and distributing shared secret keys. Surprisingly, wireless channels provide a unique source of randomness that may be harvested for such a task. The wireless signal is often subject to mechanisms such as scattering, reflection and diffraction that create multipath propagation components as shown in Fig. 1. Changes in the transmitter and receiver's positions and velocity of intermediate objects greatly influence the resulting signal, due due to constructive and destructive interference of multipath components. This fading phenomena can be viewed as an unpredictable carrier modulation driven by the channel intrinsic physical properties, which vary in different domains, as in time, distance and frequency [5].

Although multipath variability is considered as a stochastic process, it should affect similarly both legitimate parties due to reciprocity [6]. Meanwhile communication links between two parties exhibit unique channel response characteristics which become rapidly uncorrelated in both space and time [7]. The conjunction of these two factors, namely channel reciprocity and time-spatial decorrelation, permits the extraction of shared secret keys and lays the foundations for every physical layer security (PLS) approach introduced in references [8–11]. Different perspectives regarding various PLS approaches are present in current literature [12–15]. Reference [12] identifies two families of protocols, specifically based on the received signal strength (RSS) and on the channel impulse response (CIR). Furthermore, it introduces innovative schemes based on the fluctuation of the bit error rate (BER) [16], reverse pilot signalling [17], random channel hopping [18] and

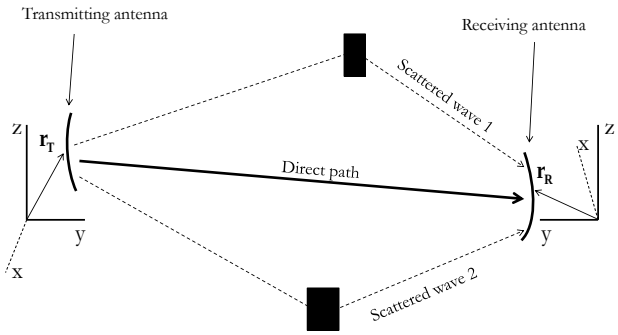


Figure 1: Multipath Signal Propagation [5]

reactive jamming [19]. Reference [13] on the other hand classifies works based on their quantisation method, their reconciliation and privacy amplification approaches together with the evaluation of the corresponding feasibility and security. In the survey [14] PLS algorithms are overviewed with a specific focus on the security threats of wireless communications at different levels of Open Systems Interconnection (OSI) model and on how they can act as both vulnerabilities and opportunities to improve secrecy rate, for example through beam-forming and the injection of artificial noise. Lastly, reference [15] provides a complete introduction to relevant challenges and solutions in both keyless security and physical layer key generation, to approaches targeting multiple-input multiple-output (MIMO) systems and the issues related to the partial knowledge of channel state information (CSI).

This paper focuses on quantisation techniques as major part of secret key establishment in physical layer security depends on the conversion of channel estimates into bit-streams, inheriting its performances and its degree of immunity against noise and imperfect reciprocity. Unlike the aforementioned surveys, the taxonomy of PLS approaches is illustrated in Fig. 2, where schemes are categorised based either on their ability to influence their contexts to increase the secrecy capacity (active harvesting) or on their passivity to rely on the existing channel conditions (passive harvesting), both of which depend on the specific characteristics they choose to quantise. Passive protocols outnumber the counter-part as they do not require special hardware, consequently promising lower implementation costs and ready-for-use solutions in current wireless networks. However, the grow-

ing demand for higher data rates pushes the adoption of multi-antennas equipped devices, fuelling the research on active techniques based on directional modulation (DM), beam-forming and the injection of artificial noise.

Another proposed contribution is presented in Fig. 3 where protocols are clustered according to the actual evaluation metrics they aim to improve. Red, blue and green boxes indicate the corresponding channel properties used by algorithms, frequency-phase, received signal strength and channel impulse response, respectively. Miscellaneous methods are excluded. Table 1 shows in more depth which part of the scheme's novelty is correlated to each key performance metric. Interestingly, the major part of protocols aims to improve the bit generation rate in order to extract keys in less time and with fewer samples. However, an inadequate bit error rate may disrupt the entire key establishment since a single uncorrectable different bit enforces the restart of the entire generation process. Furthermore, only a few schemes are interested in maximising the key entropy to cope with the poorly available randomness in low-mobility scenarios which greatly affects the overall algorithm robustness.

The rest of the work is structured as follows: section 2 introduces the concepts and the fundamental aspects of the key generation process and associated performance metrics. A brief introduction of different types of attacks and the most prominent adversarial models is also provided. Section 3 critically presents the quantisation steps focusing on different channel characteristics based on an extensive literature review of various techniques in the public domain. Finally, section 4 draws the conclusions of the literature research.

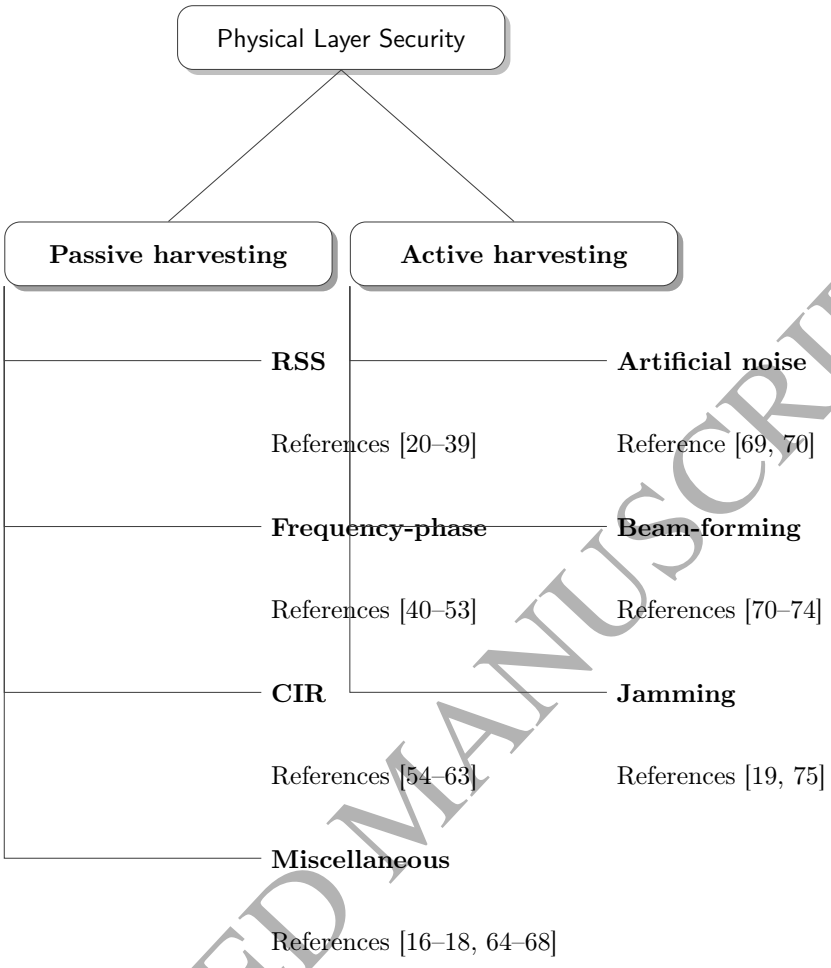


Figure 2: Taxonomy of physical layer security approaches based on nodes' harvesting abilities and the corresponding quantisation characteristics.

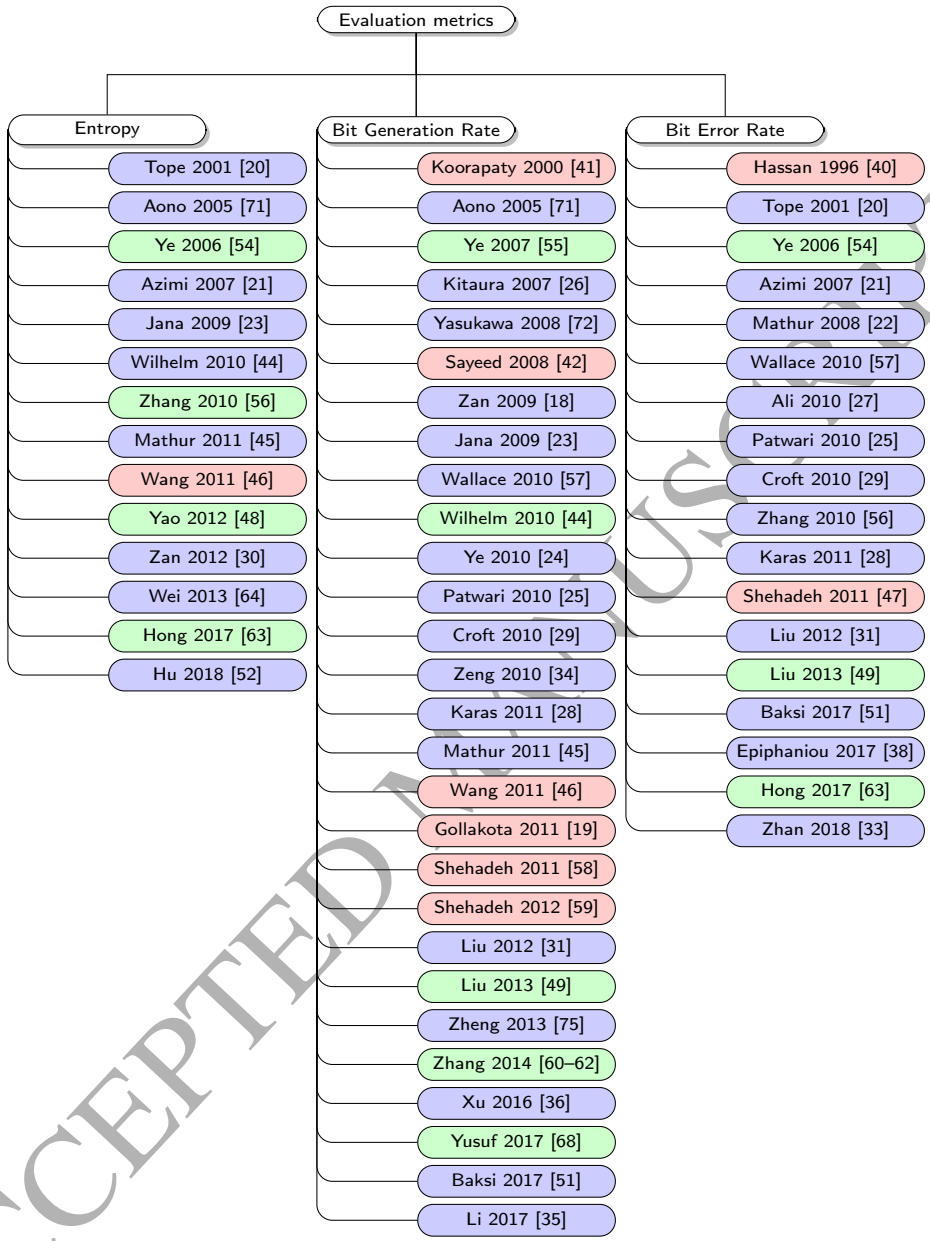


Figure 3: Taxonomy of physical layer security protocols according to their improved performance metrics. Red, blue and green boxes indicate frequency-phase, received signal strength and channel impulse response based protocols, respectively.

Table 1: Novelties subdivided by key performance metrics

| Protocol | Entropy | Bit Generation Rate | Bit Error Rate |
|---|---|---|---|
| Hassan et al., 1996 [40] | | | Quantisation of phase differentials reduces the errors due to synchronisation issues. |
| Koorapaty et al., 2000 [41] | | Extraction of multiple orthogonal frequencies separated by the coherence bandwidth. | |
| Tope and McEachen, 2001 [20] | The upper threshold removes predicable excursions. | | The lower threshold removes estimates with high probability of disagreement. |
| Aono et al., 2005 [71] | A RSS-interleaving technique randomises the key. | The beam-forming abilities of an ESPAR antenna provides superior variability also in static scenarios. | |
| Ye et al., 2006 [54] | Equi-probable quantisation ensures that all outputs have the same probability to occur. | | Minimum-mean-square-error produces a smaller BER with less key entropy. |
| Ye et al., 2007 [55] | | The Orthogonal Greedy Algorithm permits the use of CIR estimations of different paths. | |
| Kitaura et al., 2007 [26] | | Quantisation is done through the comparison the signals received by two antennas. | |

*Continued on next page*





ACCEPTED MANUSCRIPT

Table 1 – *Continued from previous page*

| **Protocol** | **Entropy** | **Bit Generation Rate** | **Bit Error Rate** |
|---|---|---|---|
| Azimi-Sadjadi et al., 2007 [21] | Fuzzy extractors correct and enhance the robustness of the keys. | | Deep fades are less susceptible to noise and interference. |
| Kitano et al., 2007 [16] | | Quantisation of BER fluctuations considers all aspects of the channel variability. | |
| Tsouri and Wulich, 2008 [17] | | Reverse piloting protocol acts as a symbol-level encryption. | |
| Yasukawa et al., 2008 [72] | | Multi-level quantisation of estimates collected by ESPAR antennas. | |
| Mathur et al., 2008 [22] | | | The level-crossing algorithm considers consecutive excursions to reduce disagreement. |
| Sayeed et al., 2008 [42] | | Quantisation of independent degrees of freedom in wideband channels. | |
| Zan and Gruteser, 2009 [18] | | Random channel hopping allows a faster key establishment. | |
| Jana et al., 2009 [23] | Thresholds are locally computed in every block of estimates. | Multi-levels quantisation compensates for the performance-loss due to privacy amplification. | |

*Continued on next page*





ACCEPTED MANUSCRIPT

Table 1 – *Continued from previous page*

| Protocol | Entropy | Bit Generation Rate | Bit Error Rate |
|---|---|---|---|
| Wallace and Sharma, 2010 [57] | | Multi-level quantisation in MIMO systems provides better performance than the single-antenna case. | Channel Quantisation Guard-band/Alternating reduces the disagreement with the use of guard-bands/alternative quantisation maps. |
| Wilhelm et al., 2010 [44] | Bit generation rate increased by exploiting frequency selectivity. | | |
| Zhang et al., 2010 [56] | Quantisation of mobility-generated CIRs | | Jigsaw Encoding emphasises how quantisation outputs are close to each other. |
| Ye et al., 2010 [24] | | | Over-quantisation improves a LDPC-based reconciliation step. |
| Ali et al., 2010 [27] | | | Large scale fading possibly avoids the need of reconciliation. |
| Patwari et al., 2010 [25] | | Multi-bit adaptive quantisation (MAQ) does not use any invalid regions or guard-bands. | Fractional interpolation compensates for estimates measured in different time instants. |
| Croft et al., 2010 [29] | | | A ranking method is introduced to remove any non-reciprocity factors due to different hardware characteristics. |
| Zeng et al., 2010 [34] | | Multi-level quantisation in MIMO systems. | |

*Continued on next page*





ACCEPTED MANUSCRIPT

Table 1 – *Continued from previous page*

| **Protocol** | **Entropy** | **Bit Generation Rate** | **Bit Error Rate** |
|---|---|---|---|
| Karas et al., 2011 [28] | | A polynomial curve is used as single threshold. | Neural network based reconciliation. |
| Mathur et al., 2011 [45] | | Quantisation of complex channel gain. | |
| Wang et al., 2011 [46] | A random initial phase-offset introduces variability even in static scenarios. | Due to the random phase, many round-trips are possible in the same coherence interval. | |
| Gollakota and Katabi, 2011 [19] | | The jamming technique renders the scheme independent from channel variations. | |
| Shehadeh and Hogrefe, 2011 [47] | | | Optimal guard intervals maintain a low BER. |
| Shehadeh et al., 2011 [58] | | Quantisation is done through phase-shifting. | |
| Shehadeh et al., 2012 [59] | | 3-Way phase-shifting quantisation is less susceptible to channel variations. | |
| Yao et al., 2012 [48] | Channels division and inter-spacing are adjusted in response to user's activity. | | |
| Zan et al., 2012 [30] | Quantisation is done on relative differences of RSS estimates. | | |

*Continued on next page*





ACCEPTED MANUSCRIPT

Table 1 – *Continued from previous page*

| **Protocol** | **Entropy** | **Bit Generation Rate** | **Bit Error Rate** |
|---|---|---|---|
| Liu et al., 2012 [31] | | | Fading trends suffers for less disagreement than absolute values. |
| Liu et al., 2013 [49] | | | Channel Gain Complement mitigates hardware and electrical differences. |
| Zheng et al., 2013 [75] | | Full-duplex jamming technique. | |
| Wei and Zeng, 2013 [64] | PID controller adapts the probing rate in response to entropy estimation. | | |
| Zhang et al., 2014 [60, 61, 61] | | CIR data is extracted from subcarriers in a OFDM system | |
| Soltani et al., 2015 [66] | | ODFM pilot tones are manipulated in order to limit adversary's estimations. | |
| Badawy et al., 2015 [65] | | Angle of arrival proved to have good performance in low SNR environments. | |
| Sadeghi et al., 2016 [67] | | In-band full-duplex devices can sense highly volatile channel states, only limited by SI-suppression circuitry. | |
| Xu et al., 2016 [36] | | Transmission and concatenation of secret keys in a group. | |

*Continued on next page*





ACCEPTED MANUSCRIPT

Table 1 – *Continued from previous page*

| Protocol | Entropy | Bit Generation Rate | Bit Error Rate |
|---|---|---|---|
| Li et al., 2016-2018 [50, 53] | | Principal component analysis decorrelates estimates resulting in a high generation rate. | Principal component analysis with common eigenvectors reduces the probability of disagreement during signal reconstruction. |
| Yusuf et al., 2017 [68] | | Signal space diversity is used to increase secrecy capacity in OFDM systems. | |
| Baksi et al., 2017 [51] | | Quantisation of complex channel gains. | Log-likelihood ratios and LPDC-based decoder compensate non-reciprocity factors. |
| Hu et al., 2017 [70] | | Random frequency diverse array-based directional modulation with artificial noise (RFDA-DM-AN) enhances the secrecy capacity. | |
| Li et al., 2017 [35] | Group-based cooperation on symmetric key generation exploiting all channels available among nodes. | | |
| Epiphaniou et al., 2017 [38] | | | Turbo-codes maintains a low BMR without the need of contiguous excursions. |

*Continued on next page*





ACCEPTED MANUSCRIPT

Table 1 – *Continued from previous page*

| **Protocol** | **Entropy** | **Bit Generation Rate** | **Bit Error Rate** |
|---|---|---|---|
| Hong et al., 2017 [63] | Clustered key mapping increases the conditional entropy of keys given the observations of the adversary. | | Rotation-based vector quantisation reduces the so-called cell-boundary problem. |
| Özbek et al., 2018 [74] | | Secrecy capacity of MISO systems is increased by actively modifying the inter-user interferences. | |
| Hu et al., 2018 [52] | The technique of frequency-hopping captures the channel frequency response and provides higher randomness. | | |
| Zhan et al. 2018 [33] | | | Curve-fitting methods remove small-scale rapid variations which cause discrepancies between parties. |





ACCEPTED MANUSCRIPT

## 2. Key generation fundamentals

According to Shannon [76], unconditionally secure communications can be obtained if the eavesdropper's observations do not provide any useful information regarding the message, without imposing any limits on processing power and time. This condition, referred to as perfect secrecy, is equivalent to a zero mutual information between the message and the key which, in turns, must have an impractical length, of at least the length of the message, as in the one-time pad implementation [77]. Shannon's considerations stem from the scenario in which all receivers sense identical copies of the transmitted signal, which may not be the generic case.

Wyner in his work [8] assumed that Eve has access to a degraded version of the legitimate channel and he proved that secure communications are possible in the absence of a secret key, under a weaker condition of secrecy. In reference [78] these results were extended to the Gaussian wiretap channel and the secrecy capacity $C_S$ was defined as the maximum achievable secrecy rate $R_S = I(W;B) - I(W;E)$ where $I(W;B), I(W;E)$ are the amount of information that Bob and Eve obtain from the message $W$, respectively. That is, the secrecy capacity is the difference between the main channel capacity $C_B$ and that of the eavesdropper's link $C_E$, thus $C_S = C_B - C_E$. Nonetheless, many techniques have been introduced to improve the secrecy capacity of a channel, as the use of multi-antenna systems to generate artificial noise and beam-forming. For an overview of such methods, readers can refer to [14, Section V].

Keyless security is based on the knowledge of the eavesdropper's channel state information which hardly holds in real-world scenarios, limiting this way its practical implementations. This constraint was relaxed by Maurer [10] and Ahlswede-Csiszar [79], who explored a new environment where Eve observes a higher quality channel in comparison to the one available for the legitimate parties, introducing a strategy for secure transmission. Maurer's idea was based on the development of a shared secret key by both Alice and Bob, over a public and insecure channel.

### *2.1. Channel reciprocity and diversity*

In addition to the background noise, the wireless medium is also subject to various effects which unpredictably modify the received signal and can be subdivided in three categories: path-loss, shadowing and multipath. Path-loss is the attenuation of the transmitted power due to distance and other propagation-related characteristics of the channel. Shadowing is also known as large scale fading and it represents the alteration of signal power caused by objects and obstacles between the

communicators. Finally, multipath or small scale fading refers to the combination of time-delayed and phase-shifted signal echoes, producing fades (nulls) and distortions [80].

The frequency-variant channel response can be written as

$$G(f,t) = \sum_{l=1}^{L} |a_l| exp(j\phi_l) exp(j2\pi v_l t) exp(-j2\pi f \tau_l)$$

where $L$ is the number of multipath components, $\{|a_l|exp(j\phi_l)\}$ their complex amplitudes with random phases $\{\phi_l\}$. Doppler frequencies $\{v_l\}$ take into account the mobility of the transmitter, the receiver and scatterers while the delays $\{\tau_l\}$ are the consequence of the different paths travelled by the different replicas of the transmitted signal [81]. Small scale fading can be limited to specific sub-regions, namely restricted time interval (RTI) and restricted bandwidth (RBW), where all the previous set of parameters $\{|a_l|\}, \{v_l\}, \{\tau_l\}$ are constant and the channel is considered wide-sense stationary uncorrelated scattering (WSSUS), leaving outside large yet slow variations such as shadowing. Moreover, there are smaller regions, referred to as coherence regions, in which the channel response is approximately constant due to the doubly underspread (DU) property that practical wireless channels possess [81, Fig 2.].

In these coherence regions two legitimate nodes can extract, in an interleaved fashion, a number of estimates from a common random source unavailable to Eve. At any given time-index the corresponding pair of measurements is highly statistically correlated according to the above reciprocity [6]. However, in real-life scenarios reciprocity is imperfect due to the asymmetries at the channel ends, interferences, phase offsets, oscillators' frequency drifts and mainly the half-duplex nature of commercial transceivers that are not able to transmit and receive simultaneously [82]. For simplicity, we refer to all these obstacles as noise whose influence requires the presence of the information reconciliation step, taken from quantum cryptography, which aims to correct such discrepancies through communication over the public channel to which the eavesdropper can freely listen [9, 10, 83].

Equally important are the variations of the channel characteristics defined as functions of the channel coherence region in the chosen metrics' domains, i.e. coherence time, coherence bandwidth and coherence length [84]. Frequency selectivity is a consequence of the irregular spectrum generated by multipath time-dispersion due to the different paths travelled by waves, each with its own delay. On the other hand, space-time variability is connected to multipath directions which constructively/destructively alters the resulting signal even with small movements of the receiver

[7].

The simultaneous presence of highly correlated behaviours inside the coherence region and the unpredictable diversity outside it gives birth to a difference of mutual information between legitimate parties and adversaries, which is considered as a shared source of randomness successfully harvested for the extraction of a symmetric key. Frequency diversity is explored in reference [44] and improved by [45, 48, 49, 52, 85], while the spatial domain is investigated in references [57, 86–90].

In all these approaches, the quantisation stage plays an important role in extracting the wireless channel information needed in consecutive steps for the secret key establishment. The challenging aspects of the quantisation process are mainly attributed to the contrasting relationship between the rate of generated bits, their entropy and robustness and their correlation at both communication ends, which is trivially related neither to the specific choice of the channel characteristics nor to the scheme's parameters [22, 91].

### *2.2. Evaluation metrics*

In order to compare and contrast different key generation protocols, it is necessary to introduce the corresponding performance metrics. These are: 1) the randomness or the entropy of the key, 2) the bit mismatch rate (BMR) and 3) the bit generation rate (BGR) [23]. In certain studies, both BGR and BMR are leveraged in order to obtain the key generation rate (KGR) and the key disagreement rate (KDR) [64, 92]. Similar to any conventional cryptographic method, in PLS algorithms the key must not have any statistical defects in order to maximise the uncertainty from Eve's point of view. Given a key of length $N$, the associated entropy is defined as:

$$H = -p_0 log_2 p_0 - (1 - p_0) log_2 (1 - p_0)$$

where $p_0$ is the posterior probability of bits being zero from Eve's knowledge [93]. Therefore, the key must expose properties that a truly random sequence would probably exhibit as expressed in reference [1]. Fifteen tests are provided by the National Institute of Standards and Technology (NIST) [94] which verify different aspects, such as the frequency of symbols' occurrences, the presence of long runs and other periodic features. The bit mismatch rate is an evaluation metric strictly linked to the quantisation step and its parameters and it is defined as the ratio of mismatch bits to the total number of generated bits [23]. Low levels of BMR confirm the resilience of the quantisation scheme against the noise and the asymmetric differences of the channel. In contrast, high BMRs

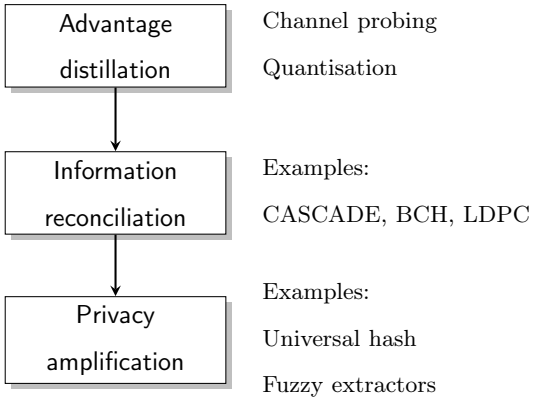


Figure 4: The secret key extraction process

could greatly influence the overall performance of the systems since a single uncorrectable bit may force the reject of the entire sequence and the restart of the full process.

The bit generation rate is defined as the number of secret bits generated per unit time or per sample [23] which depends on both protocols' properties and on environmental characteristics, such as nodes' movements and multipath richness. Higher values of BGR indicate the faster ability of two nodes of establishing a key of the desired length. This metric acts as a global performance indicator by incorporating all contrasting aspects of the secret generation process. In fact, the distillation stage aims to increase its throughput by harvesting increasingly detailed channel characteristics, whilst the information reconciliation and privacy amplification phases unavoidably decrease it by dropping erroneous and predictable bits, respectively.

### *2.3. The secret key generation process*

For the sake of simplicity, the process of secret key generation can be divided in three fundamental tasks (see Fig. 4): the first one, called advantage distillation [10, 95] focuses on extracting information available only to the legitimate parties. This initiates with a channel probing task, also referred to as beacon exchange, which consists of the interleaved exchange of probes by Alice and Bob in the process of gathering their corresponding estimates. Mathematically, the measurements are defined as follows:

$$\hat{H}_A(t_A) = h(t_A) + w(t_A)$$

$$\hat{H}_B(t_B) = h(t_B) + w(t_B)$$

where $h(t)$ is the reciprocal channel response, $w(t)$ the additive white Gaussian noise and $\hat{H}_X(t)$ the noisy estimates. The duration of the probing phase is proportional to the desired key length, whilst the probing frequency depends on the dynamic properties of the channel. In fact, in order to sense correlated estimates both Alice and Bob must collect their measurements inside the coherence time $T_c$ of the channel that represents the time duration over which the channel impulse response is considered as static.

In wireless medium the coherence time is strictly connected to Doppler effects due to nodes' movements [96]. Specifically, the coherence interval $T_c = 1/f_{max}$ is the time domain dual of the maximum Doppler frequency $f_{max} = f_{Tmax} + f_{Rmax} + f_{Smax}$ where the latter includes the frequency contributions of the transmitter $f_{Tmax}$, the receiver $f_{Rmax}$ and the mobile scatterers $f_{Smax}$ [81]. A fast probing rate will easily result in redundant estimates which are not suitable in the generation of a key and must be re-sampled in order to extract a distinct measurement for each coherence time. In rare cases probing could be done continuously, for example by injecting an initial random phase as in reference [46].

The majority of the protocols use a fixed probing rate which does not adapt to dynamically changing channels, limiting their capacity to exploit any added randomness or in some cases extract useless correlated estimates. In reference [60] the relationship between the percentage of coherence time and the randomness of the key is investigated and authors claim that the most widely used sample interval of 50% of the coherence time is not sufficient to guarantee enough statistical robustness of the key. An indirect approach, proposed in reference [64], assesses the probing rate by evaluating entropy, through the Lempel and Ziv complexities associated to the finite-time size sequences, in order to drive a proportional integral derivative (PID) controller which dynamically tunes the frequency.

Channel estimates are then converted into binary strings in a successive quantisation step which holds a primary role in the entire bit extraction process, thus greatly influencing the overall performance of the system. The output at this point has the potential to become the shared secret key after passing through further steps. For this reason, every quantisation scheme is evaluated against two contrasting metrics, as in the bit generation rate and the bit mismatch rate, in an effort to maximise the former and minimise the latter. Although simple and easy to implement, the use of uniform quantisation [97] is to be avoided because BMR rapidly increases with the number of

quantisation intervals [56].

The number of thresholds constitutes another useful classification. In fact, even if quantisation itself does intrinsically reduce the amount of information, a lossy or censor scheme drops values that fall in specific invalid regions in its effort to minimise disagreement probability. On the other hand, lossless schemes convert every estimate with single or multi-thresholds (see Fig. 5 and 6).

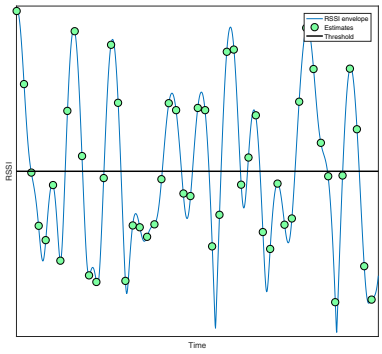


Figure 5: An example of RSS-based lossless quantisation: every channels estimate is used through the comparing with a unique threshold.

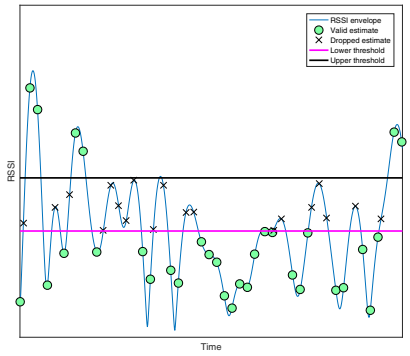


Figure 6: An example of RSS-based lossy / censor quantisation: channels estimates between thresholds are dropped to reduce the bit disagreement rate.

After quantisation, bit-streams pass through an information reconciliation block which has the role of correcting any bit disagreement. Its implementation varies from error correction codes to fuzzy techniques. The majority of protocols uses an algorithm called CASCADE [83] in which Alice randomly permutes the bit sequence and exchanges with Bob the parity check information. Bob, on the other hand, permutes his bits in the same way and checks his parity trying to correct any potential discrepancies. This process can be iterated to increase the probability of success. At a later time, researchers proposed new techniques with better reconciliation capabilities, while minimising the potential information leakage to an adversary [56, 71].

At this point, Alice and Bob's bit-streams should be identical otherwise the key generation process restarts. However, these sequences are not yet ready to be used as a key. Before that, it is necessary that vectors do not reveal any of the information used in their creation. In fact, information reconciliation through public discussion reveals useful information on eavesdropper Eve, weakening the protocol robustness. The step of privacy amplification aims to increase key

entropy, for example by applying a universal hash function which maps $n$ bits to sequences of lesser length $k < n$ of which Eve does not have any details [98]. In other protocols, privacy amplification is obtained by XORing the sequences generated from different sources, as in the case of different antennas in a MIMO system [34]. The role of privacy amplification is what makes lossy/lossless classification even more interesting. Lossy schemes sacrifice a high generation rate to remove statistic defects from the bit-streams, which are directly used as a secret key without the need for privacy amplification. Applications of this approach are in references [20, 22, 71]. In contrast, lossless schemes produce a higher bit extraction rate but rely on privacy amplification to increase the entropy of the resulting sequence.

### *2.4. Feasibility of physical layer security approaches*

Deployment costs and resilience against attacks are important factors to bear in mind while evaluating the feasibility of security infrastructures, especially when the size and the topology of the network are continuously changing. In contrast to conventional cryptography, PLS-based methods do not require additional hardware as the keys are extrapolated from the channel itself, whilst conventional approaches usually require additional hardware in order to contain and protect all the keys to be used in future communications. On the other hand, PLS schemes have to continuously evaluate channel properties, introducing a conspicuous operational cost. In reference [99] authors argued that the latter possibly annihilates the interest for adoption by the industry but they do not seem to consider the computation and network overhead caused by public key algorithms during the signature verification.

Attacks against PLS can be categorised into either active or passive. Passive attacks are considered by all proposed schemes which consist in the ability of Eve to fully listen to the communication between Alice and Bob at the same instant it takes place. Robustness against passive attacks is a direct consequence of the wireless space-time variability, which renders adversary's estimates uncorrelated from the corresponding ones sensed in the main channel. This crucial point is further investigated in reference [100] where the diametrically opposed scenario in which Eve has full knowledge of the context (for example, the position and the mobility of every object) it is considered and equations have been derived to compute the channel impulse response as Alice or Bob would observe it. Despite this interesting, different point of view, the initial assumption is too strong and utopian in real-world scenarios.

On the other hand, active adversaries have the ability to interfere and modify the communication context. In reference [101] the adversary, Mallory, exploits the superposition characteristic of the wireless medium, by injecting malicious packets and then destroying the legitimate ones with jamming techniques [102].

Let $r_a^b$ be the response of the channel during a transmission from Bob to Alice which coincides with $r_b^a$ not considering non-reciprocity factors. In addition, let $r_m^a, r_m^b$ be the responses of signals received by Mallory from Alice or Bob, thus implying $r_m^a \approx r_a^m$ and $r_m^b \approx r_b^m$. The key idea is that even if the adversary does not know how exactly probes are received by the legitimate parties, he does know that their differential $d = |r_m^a - r_m^b|$ will be preserved. In the case that Mallory detects a high differential, this constitutes an excellent opportunity to inject estimates for Alice and Bob by sending a signal of maximum magnitude to the node with the highest RSSI and a minimal powered packet to the other end, forcing them to disagree, thus sabotaging their generation process. To be more precise, disagreement on more bits may be needed to disrupt the entire process, but this number must be kept to a minimum, in order not to be detected by statistic countermeasures. On the other hand, a low differential means that injected packets cause a similar channel response to Alice and Bob, presenting an opportunity to generate the same bits through their corresponding quantisation steps. When Mallory detects such a condition, he saves the received RSS value and then sends spoofed probes to both Alice and Bob. According to the small differential, ideally zero, Alice and Bob may choose this injected excursion to generate bits, thus letting the adversary to recover part of the key after estimating quantisation levels by scenario-based guessing or better by a specific setup phase.

To protect the previous schemes from such an attack, reference [30] proposes an improvement consisting of RSS values not directly used as quantisation inputs but replaced with relative differences. In the first step, Alice and Bob collect estimates at their maximum probing rate, split them into segments and then remove slow fluctuations, which dominate the channel variations in static environments by subtracting a moving average. In every segment the first estimate is used as a single threshold to emit bits according to the sign of delta values. Comparing to [22], the use of relative differences makes this scheme immune to attacks as described in reference [23] because of its ability to generate high entropy bits, even if RSS values are globally very low. Moreover, the extraction rate records an increase of 200% mainly because an agreement between parties does not require the presence of contiguous excursions.

A formal model of the adversary has been proposed in reference [103] based on the probability of knowing any of the estimates. This probability is considered as part of the privacy amplification to include the information leaked during both quantisation and information reconciliation stages.

Assuming that the probability is unknown to legitimate parties, authors claim that entropy estimation of the key is irrelevant, if it is done from Alice or Bob's points of view. In fact, Alice or Bob may consider random a sequence which has zero entropy for Eve. Protocol designs should use the entropy estimation according to the adversary, proven to be very complex. The authors assert that the generation of secret shared keys could be viewed as the synchronisation of two pseudo-random number generators (PRNG) at legitimate nodes. Following this similarity, they expect that the existing knowledge about PRNG will strengthen the robustness of wireless security approaches. In their study, they propose to divide the extraction phase into two parts, referred to as Entropy Harvesting and Entropy Management. The former has the objective to continuously gather estimates from the channel and to collect them even if the key does not have to be generated. Entropy Management will peek from that poll to feed a robust PRNG which maintains the state and generates the keys as needed.

In the majority of schemes in literature, there is also the assumption of the presence of an authenticated channel which implies that the identities of Alice and Bob have already been verified prior to the information reconciliation step. Nevertheless, this assumption is unrealistic because authentication requires the exchange of a security key which is the result of the successive steps. However, only in a few studies these issues are addressed. In reference [22] Eve tries to masquerade Alice's role by sending a sequence of indices to Bob. Following from the uncorrelated behaviour caused by distance, these indices are likely to contain invalid positions that can be detected by statistic countermeasures, i.e. by using a correlation threshold.

## 3. Channel characteristics and quantisation schemes

Physical layer security is linked to the channel characteristics which are used as sources of randomness for secret keys generation. In contrast to traditional security, where the channel is assumed to be ideal and error-free, here the imperfection and variability of its characteristics are essential to extract high entropy keys [104]. As pointed out in [105], many of the following approaches rely on a single source of randomness, usually the carrier magnitude and a binary quantisation space made up of thresholds which are applied on absolute or differential estimates. However, channel

characteristics are not mutually exclusive allowing the simultaneous estimations of multiple sources to raise the bit extraction rate, as in [45] where both channel gain and phase are collected. In these cases an additional step, namely Fusion Operation [106], needs to be placed right before the quantisation step, working on physical estimates, or located after it, merging the resulting bit-streams. Noteworthy, the statistical independence of estimates from different sources does not imply the non-correlation of corresponding errors and errors' bounds; for example, as argued in [105], the phase highly fluctuates at low amplitudes, while the reverse is also true. This suggests that the design of quantisation space is neither homogeneous nor uniform, hence needs to be adapted to context specific behaviours, empirically determined.

Received signal strength, channel impulse response and frequency-phase are the most popular channel parameters used in estimates. More specifically, received signal strength indicator (RSSI) is by far the most used approach because its value is available in all out-of-the-shelf transceivers on a frame basis hence, dramatically reducing design and implementation costs. Frequency-phase and CIR-based approaches are more resilient to attacks, as well as being able to generate long secret keys depending on the uniformly distributed nature of the former, as well as to the CSI details given by the latter. In work [65], the exploitation of the angle of arrival (AoA) manifests good performances at very low signal to noise levels, whereas other characteristics tend to be weak. However, these techniques involve both computational and hardware complexities which may not be sustainable in common scenarios (see Table 2).

### *3.1. RSS based methods*

In their work [20], Tope et al. introduced a protocol based on the evaluation of signal attenuation caused by multipath channels extracted from the envelope of received packets. Channel estimates are not directly quantised but instead, arrays of variations are generated by subtracting half values from the other half, in order to remove the predictable slowly changing component due to path-loss, which is correlated to the distance between the transmitter and the receiver. Two fixed thresholds drop the lowest and highest values, to reduce the probability of disagreement and to improve key robustness, respectively. The proposed scheme does not take imperfect reciprocity into account, stating that the correlation between estimates could always be increased by choosing a sufficient fast probing rate. Furthermore, low-mobility or static scenarios produce negligible envelope variations, which are likely filtered out by the low threshold, resulting in a reduced global performance.

Table 2: Comparison of common sources of randomness

| Attribute | Complexity | Resilience | Cons | Pros |
|---|---|---|---|---|
| RSS | Low | Low | Extraction rate and key entropy depend on mobility | Reduced implementation and deployment costs |
| Freq-Phase | High | High | Require specific hardware and subject to synchronisation issues | Robust in both static and dynamic environments; usable in group key generation |
| CIR | Medium | High | Suffers from imperfect reciprocity and require advances channel estimation methods | More detailed CSI hence higher generation rate even in static scenarios |
| AoA | High | Medium | Hard to estimate | Good performance even at low SNR |

Even if thresholds decrease mismatch probability, as well as the predictability of the generated bits, they drop all the same values outside permitted ranges. Therefore, they fail to exploit estimates that may potentially improve the bit extraction rate. This fact suggests that quantisation performances are strictly dependent on the choice of the physical characteristics of the channel used for estimates and the specific selection of parameters (thresholds), which are often made only through empirical evaluations, hence not necessarily optimal.

An automatic thresholds method has been proposed in [21] where the lossless scheme is based on the detection of deep fades that are local minima of the signal, considered to be less subjective to disagreement. In this approach, bit-streams are generated by comparing the estimates with a single threshold, set by an automatic gain control circuit (AGC), rendering it independent from the variability of signal power and its attenuation. Deep fades are represented by sub-sequences of a sufficient number of 1-bits, referred to as runs. Possible disagreements between Alice and Bob's fade locations are only imputable to bits shifts and differences situated either at the beginning or at the end of a run. This fact, together with the knowledge of the deep-fades rate, deriving from the channel statistics and the Rayleigh model, shrinks the search space which can be explored by Bob to find the vector that generated the hash received from Alice, thus extracting the secret key. Information reconciliation is provided by a fuzzy reconciliation technique which simultaneously corrects the disagreements and enhances randomness of the streams.

Due to the use of deep fades, previous scheme is less susceptible to noise and interference, but the overall entropy of the key still depends on the movements of nodes involved in the communication. That strongly dictates the artificial creation of interference to introduce the necessary variability to extract a secret key. Unfortunately, evaluation is limited to simulation and theoretical analysis, not revealing the relationship between the key generation rate and the choice of system parameters.

Inspired by the previous scheme, the protocol proposed in [22] provides authentication and gives a detailed analysis of the relationship between the choice of quantisation parameters and the resulting performance. A windowed average is subtracted to remove shadow fading (or large scale fading) effects which introduce slow, yet substantial alterations to the signal power. Quantiser is based on two thresholds calculated using average $\mu$ and standard deviations $\sigma$ computed on arrays of estimates $\underline{\hat{h}}$

$$q_{\pm} = \mu(\underline{\hat{h}}) \pm \alpha \cdot \sigma(\underline{\hat{h}})$$

and a quantisation function $Q(\cdot)$ defined as

$$Q(x) = \begin{cases} 1, & \text{if } x > q_{+} \\ 0, & \text{if } x < q_{-} \\ \text{dropped} & \text{otherwise} \end{cases}$$

In this protocol, as well as in all level crossing schemes, the key robustness is best achieved in Rician and Rayleigh fading models because of their symmetry around the distribution means, hence an equal probability of having positive and negative excursions. Quantisation parameters are chosen starting from the desired probability of key disagreement, which in turns depends on the probability for which the two sequences disagree on a single bit. A more prudent choice of parameters leads to a reduction of the key generation rate, which in turns, is limited by the level-crossing rate in Rayleigh model in the order of maximum Doppler frequency [96]. In other words, one cannot indefinitely keep on increasing the probing rate to raise the secret key generation rate because the latter saturates at the maximum Doppler frequency. Nonetheless, if we increase the latter while keeping a fixed probing rate, the key generation rate will again decrease. These behaviours indicate that probing rate and other system parameters have to be chosen according to the dynamic characteristics of the channel itself. To further reduce BMR, the scheme quantises estimates only if they are contained in a sequence of $m$ excursions above or below the corresponding thresholds, with $m$ a fixed system parameter.

This constraint has been removed in reference [39], obtaining a slightly higher generation rate at the costs of an increased bit mismatch rate. Nonetheless, in [38] the application of turbo codes efficiently maintains a low BMR during the analysis of a standard quantisation scheme in vehicle-to-vehicle scenarios with three-dimensional scattering and scatterers' mobility. Previous approaches are based on fixed thresholds and they have failed to achieve fast key generation rate with high entropy because of their susceptibility to static environments [20, 21] and the sacrifice of some bits in return for a stronger robustness [22].

Inspired by [22], the scheme introduced by authors in [23], namely Adaptive Secret Bit Generation (ASBG), dynamically calculates its quantisation thresholds in every block (of configurable size) of channel estimates. Furthermore, instead of asking for continuous excursions of sufficient length, here the quantisation is applied at each measurement, delegating to the privacy amplification step the task of removing bit correlations. To compensate for this information loss, ASBG tries to extract more bits from a single estimate, dividing the entire RSS interval in noise-limited number $n \sim 4$ of levels. As disagrements usually involve adjacent quantisation bins, Gray codes [107] are preferred to increase the probability of resolving such mismatches within the reconciliation step based on CASCADE [83]. The authors elaborated further their analysis in reference [32] where they explored the key generation possibilities offered by multiple-input multiple-output contexts, with the concurrent introduction of an iterative distillation step which eliminates measurements that are likely to disagree between the parties. They also analysed the performance of different schemes in real-world scenarios which gave the opportunity to summarise the pros and cons of RSS-based approaches. The specific threat model includes an adversary able to control part of the environment to render the estimates more predictable, as in the case of moving intermediate objects.

In [24], over-quantisation is used to improve a reconciliation step based on a low-density parity check code (LDPC) fed by log-likelihood ratio estimates. In fact, even if over-quantised bits are independent of the regular ones when an equiprobable quantisation is applied, both of them statistically depend on Bob's estimates. This increased amount of mutual information reduces the required number of bits in the syndrome needed by Bob, rising the secret key rate. A similar reconciliation approach is also used in [51] in a phase-based scheme.

A more sophisticated adaptable threshold has been proposed in [28]. In this scheme, each transceiver creates a least-square polynomial curve whose degree is chosen according to estimates'

length and the Doppler shift. This curve serves as a unique threshold for quantisation, which is able to detect fades of smaller depths in contrast to the constant thresholding method. Simulations demonstrate that a high level crossing rate (LCR) is achievable with a relatively low degree of the polynomial, in both Rician and Rayleigh fading models. Agreement rates are also improved via a neural networks-based reconciliation, which authors plan to also use in the field of authentication and user verification.

A neglected possibility of previous schemes is the mitigation of imperfect reciprocity, commonly considered as a consequence of uncontrollable and unpredictable noisy factors, mostly the non-simultaneous directional measurements. In this attempt, in reference [25] a framework referred to as High Uncorrelated Bit Extraction (HRUBE) was introduced composed of three parts: interpolation, decorrelation and adaptive multi-bit quantisation. In the first step, a technique called Fractional Interpolation, consisting in the application of cubic Farrow filter to interpolate the channel measurements, moves the latter as if they have been made at the same time instant. In the following step, a Karhunen-Loéve transform (KLT) decorrelates vectors' components, which are then converted into bits in an Multi-bit Adaptive Quantisation (MAQ) scheme.

The absence of guard intervals encourages the design of a dynamic technique, to obtain a low error rate when measurements are close to the threshold, where it is likely that the other part has already exceeded it. In MAQ, at any time the leader node has two quantisation variants at its disposal, to choose one with the least probability of generating a mismatch. Even if the latter still happens, the usage of Gray codes limits such a disagreement in only one bit. The lack of guard intervals or invalid regions allows HRUBE to achieve a high key generation rate of 10 bits/sec with a 0.54% bit mismatch rate and even better results of 22 bits/sec with a higher disagreement rate 2.2%. Unfortunately, after the application of KLT, estimates can still be dependent on high-order cross moments which implies that an adversary may be able to exploit this statistical defect and predict specific values, a possibility that requires further research.

In reference [29] the Adaptive Ranking-based Uncorrelated Bit Extraction (ARUBE) protocol has been introduced as an improvement over HRUBE with the aim to remove any non-reciprocity factors due to different hardware characteristics. The ranking method has a dual purpose: firstly, it makes the process less related to the specific fading distribution and secondly, it normalises the scales of different RSS-circuitries and various levels of signal powers. The added robustness also brings an increment of 30%-60% bits per sample, in contrast to the previous protocol, reaching a

total of 40 bits/sec with a low disagreement probability.

Another scheme leveraging Farrow filter to address imperfect reciprocity is presented in reference [31] where the problem of the collective extraction of a random key from a group of nodes is analysed. Clearly, real RSS values must not be transmitted during the key agreement phase and moreover, individual members of the group could be outside the communication range of others. Consequently, authors designed a relying technique to assist the key generation, introducing a new metric, named Difference Of Signal Strength (DOSS), which is the difference among RSS indicators measured at one node via different radio channels. Sharing this metric will not introduce security weaknesses because an adversary may not recover the exact RSS estimates. The idea underlying this scheme is that all members use the RSS values between two randomly chosen nodes as the shared source of randomness to extract the common key. Even if they do not know these values by direct estimate, they know that differentials (i.e. DOSS values) will be preserved and shared during the communication, which somewhat sends back the technique to the base of man-in-the-middle attack [101].

According to the consideration that RSS measurements are more likely to agree on positive or negative trends instead of absolute values, the scheme chooses to quantise fading trends to reduce the high bit mismatch rate associated to any multi-levels approaches, an idea at middle distance between a standard approach and a full differential one as proposed in reference [30]. After a first step of time interpolation to address non-simultaneous probes, estimates are browsed in the search for continuous variations with the same polarity, i.e. trends, which are immediately quantised. Values outside these monotone sequences are not dropped but quantised by a standard multi-level approach as proposed in reference [25]. Similarly to the latter, an increase of the number of quantisation levels still leads to a corresponding increase in BMR, however, this drawback is limited by the high number of measurements exhibiting fading trends.

Instead of transmitting RSS differential values, reference [36] proposes a way to secure the distribution of keys among nodes. Starting from the simplest scenario, three nodes generate pairwise keys $K_{1,2}, K_{2,3}, K_{3,1}$ using a standard one-to-one training process. After that, each node splits the keys it possesses into two independent segments and sends their composition to the other nodes. For example, node 1 possesses the split keys $K^1_{1,2}K^2_{1,2}, K^1_{3,1}K^2_{3,1}$ and sends $K^1_{1,2} \oplus K^1_{3,1}$. After a full round-trip, all nodes can concatenate the three keys, obtaining the final group key. The scheme has been extended to more complex network topologies, however, it seems not to be able to exploit all

the channels available among nodes.

To achieve this objective, reference [35] starts from the idea that groups of nodes can be treated as virtual wireless devices with multiple antennas, as long as they are interconnected in a secure and smooth fashion. Each group has its own representative which is the primary controller in the process of adding a new legitimate node. The latter exchanges probes with the entire group, measuring the channels among it and all members. Simultaneously, group's participants estimate the channels to the new node and send their results to the controller, which is now able to exploit an increased RSSI data density. The proposed collaborative scheme accumulates this data faster than serial approaches with the added benefit of having the joining node with low energy consumption since it can multicast its probes. However, the group (especially the representative) consumes more energy, a fact that can have a wide impact if it is composed of resource-constrained nodes. Moreover, further analysis is needed to take into account possible active adversaries as the system seems to be prone to jamming attacks or packet injections.

In [33] a curve-fitting method is proposed to reduce the number of discrepancies between the legitimate parties. Spearman correlation coefficient is used to evaluate the statistical dependence of different tests, demonstrating that the correlation of whole trials is higher than the same metric on smaller intervals, which suggests the presence of correlated primary patterns accompanying with different small-scale rapid variations. The removal of the latter is done by the application of smoothing/curve-fitting techniques, improving both mutual information and correlation. The work explored curve-fitting based on Fourier series and a moving average but besides their difference in complexity, it is not clear how the choice affects the evaluation metric, especially when it comes to the key entropy. In contrast to a standard censor scheme, the multi-level quantisations convert all samples into bits and a high number of levels $\sim 16$ are usable keeping the mismatch probability under the capacity of the CASCADE algorithm.

According to the fact that wireless signal behaves independently in different antennas, nodes in a MIMO system are able to harvest more mutual information, thus improving the secrecy throughput. Intuitively, MIMO systems can scan more sub-channels and they are more likely to find some of better quality (i.e. more shared randomness) than the single-antenna ones, whose combination has a higher agreement rate. In reference [34] tests revealed that the extraction rate is four times higher than what is achievable in the single-antenna mode. The increased amount of secrecy capacity seems to highly depend on the specific couple of antennas considered and on the order in which each pair

is probed. Unfortunately, this dependency and the design of a more elaborated protocol aiming to adapt the quantisation scheme to high-randomness channels, remain open to further research.

In [26], different signals received by different antennas are measured and compared, generating bits according to their relative variations. In other words, the current quantisation thresholds are replaced with the estimates coming from the other inputs. The simulation shows that the protocol requires an signal-to-noise (SNR) ratio of 20 dB and additional techniques to achieve a sufficiently low bit disagreement rate.

Providing for the lack of multiple antennas systems, wireless relays can be used to introduce randomness in static scenarios, acting as shared additional antennas. In [37] an untrusted relay is connected to the legitimate parties through time-variant channels, for example due to its mobility. The key generation process starts with Alice sending a randomly chosen variable to both Bob and the relay, however, only Bob is able to determine the original variable since the reciprocal channel is static. The relay then forwards the received signal to Bob which, in turns, extracts the original signal and obtains the estimate of the channel connecting the relay, thus exploiting its randomness. Simulations show that the introduction of the relay allows the extraction of keys in static environments, at the cost of an increased BMR.

The removal of large-scale fading is a widely used technique in RSS-based approaches because slow fading is predictable and leads to low entropy bit-streams which limit the robustness of the resulting secret key. Nonetheless, there are specific scenarios where these slow differentials are not only interesting but also optimal, considering the associated bit mismatch rate that results much lower than the one related to the faster component. This is evident in reference [27] where physical layer security is applied in body area networks composed by small sensors positioned on the human body to record vital signals with the ability to transmit them to a base station for filing and further analysis. RSS has been preferred to other characteristics, such as phase and channel impulse response, for its feasibility in limited energetic and computational power. In contrast to the majority of approaches, slow fading has proven to be acceptable by contrasting the intrinsic predictability and low entropy with down-sampling, hence lowering the rate of bit extraction. The generation process includes a Savitzky Golay filter which isolates the slow variation and a standard quantisation scheme similar to the one introduced in reference [22]. The main advantage of using large-scale fading is the possibility to avoid the information reconciliation step entirely or use a simple one instead, such as a single parity bit for a small block length empirically extrapolated.

However, the lack of authentication renders this approach very weak against active attacks, such as jamming and packet injection, which are unfortunately not taken into account but left aside for future work.

### *3.2. Frequency-phase based methods*

Received signal strength is an attractive channel characteristic because of the simplicity in its use but as noted in the previous section, all RSS-based schemes suffer from poor performance in static environments. Node movements (and the various objects between them) are necessary to reduce coherence time by increasing the Doppler spread which in turn, gives the upper bound of the bit extraction rate for sufficiently uncorrelated estimates in the Rayleigh fading model [45]. Nonetheless, the reciprocity principle does not only hold for RSS, but it is also extended to the full channel state information (CSI), expressed as a complex number representing the amplitude and the phase-offset applied to the transmitted signals.

Channel phase has the fundamental advantage of being less predicable in contrast to RSS values which can be influenced by an adversary by manipulating (part of) the environment to introduce interferences and to move intermediate objects. In fact, given a transmitted signal in the form $A(t)cos(2\pi f_c t + \phi(t))$, where $A(t), \phi(t)$ are the time-variant amplitude and phase and $f_c$ the carrier frequency, the channel modifies it introducing time-variant attenuation $H(t)$ and phase-offset $\theta(t)$. The resulting signal $H(t)A(t)e^{j(\phi(t)+\theta(t))}$ evidentiates the multiplicative nature of the amplitude which Eve can influence, however, it also shows the immunity of the phase, being additive and cyclic on a $2\pi$ period.

A first attempt in using phase as a source of randomness was done in reference [40] where authors proposed a strategy based on the differential phase of two identical sinusoids at different frequencies and error correcting codes to reduce BMR. Phase differences are preferred to the direct quantisation of the absolute values because they reduce the non-reciprocity factor caused by the internal local oscillators which are hardly synchronised with all nodes. Arbitrarily long keys could be generated by iteratively repeating the process. Furthermore, the authors generalised their protocol in reference [41] where the phase differentials are extracted from sinusoids, which are emitted at orthogonal frequencies separated by at least the coherence bandwidth of the channel to ensure statistical independence.

A similar technique was adopted in [42] where the keys are synthesised through the quantisation

of a number of degrees of freedom (DoF) which are obtained by splitting the frequency band into independent coherence bandwidths. Inspired by the work in reference [40], the document introduced a theoretical analysis of the probability of phase agreement as a function of both the signal-to-interference-and-noise ratio (SINR) and the number of quantisation intervals. Not surprisingly, both the theory and the simulation agree on asking higher SINR to achieve sufficient agreement probability with an increasing number of quantisation levels.

In [45], phase differentials and amplitudes are exploited as two statistically independent sources. Probing is done at every fixed interval greater than the coherence interval, hence the bit generation rate is still limited to the channel temporal variations which can be increased by a factor of 3-4 by moving the transceivers. Complex channel gain has also been exploited in [51] where a one-bit quantisation is applied in both amplitude and phase. Log-likelihood ratios (LLR) feed a LDPC decoder to compensate non-reciprocity factors which significantly influences BMR in lossless protocols. Since these ratios are calculated as a function of the difference between Alice and Bob's current measurements, they do not require any knowledge of channel statistics, hence they don't need time-consuming operations such as the variance estimation by taking advantage of the symmetry of channel gain probability density function. LLR calculation itself is computationally complex, however, experiments show that a faster approximation based on BPSK-LLR is a feasible alternative in low SNR environments.

In its try to further improve key generation rate beyond coherence time saturation, the work in [46] injects random initial phases in each extraction round-trip, proposing a scheme which is also scalable for groups of nodes. To avoid the complex partial exchange of estimates, typical in RSS-based group key generation as in [31], this protocol uses the sums of phase offsets, taking advantage of the fact that they are identical in each node after a clockwise and anti-clockwise round-trip done in the same coherence interval. The resulting phase is then converted into bit-streams by multi-level quantisation. One of the most significant improvements in this scheme is the possibility to do many round-trips inside the same coherence interval because the choice of random phases provides for the lack of entropy in static environments as well. The ability to scale with a group of nodes is also appealing, however, the number of members is limited by the bit error rate and the signal-noise ratio associated with the channel. On the other hand, this protocol assumes that all nodes are synchronised, that is they share a standard time reference. In particular scenarios this can be unrealistic, as the use of local and independent oscillators introduces unpredictable and

unmanageable phase offsets. Moreover, the algorithm assumes the availability of an authenticated channel, where the identity of the nodes has already been previously verified and therefore it is not threatened by man-in-the-middle attacks.

In the previous scheme, the quantisation scheme does not have any invalid region, hence it can extract bits from each estimate. Nevertheless, estimates in regions' boundaries can easily lead to disagreement between communication parties and guard intervals are recommended to maintain a low BMR, as proposed in [47]. Intuitively, larger boundary regions will lower the probability of mismatch, while they simultaneously decrease the bit extraction rate as more estimates are likely to be dropped. Consequently, the error probability is expressed as the condition in which two correlated estimates are situated in different quantisation regions, depending on the tap-to-noise ratio (TNR). Starting from the TNR, one can choose optimal values of the guard angle and the number of quantisation sectors, in order to achieve the maximum number of extractable bits through phase-shift-keying (PSK) demodulation.

One of the firsts attempts to exploit frequency diversity was done in [43, 44] which started from the consideration that channel fading is frequency selective and sub-channels independently induct small, yet not negligible phase variations which could potentially generate significant and unpredictable changes in the amplitudes of the resulting signals. The proposed algorithm extracts arrays of measurements from each frequency and calculates their averages which are then converted in a multi-level quantisation. Disagreements are not addressed by error correcting code but instead, they are reduced to a minimum with the choice of a set of tolerances based on the variance of the measurements and a feedback from the previous generation attempt. The exploration of sub-channels has the immediate consequence of multiplying the bit generation rate, which can be further improved by raising the number of quantisation levels with the aid of a more precise and costly hardware. Inter-dependence between frequencies has been evaluated with a stochastic model that showed how the bit extraction rate does not monotonically grow with the bandwidth and that a larger channel spacing can be another way to improve the scheme's efficiency.

Authors in [48], adjusted the number of channels and their inter-spacing in response to the user's activity. Experiments showed that in high activity contexts the reduced coherence time is best explored by sampling a limited number of channels with an adequate channel spacing. On the other hand, low activity scenarios involve long stable communication paths, which allow the harvesting of a greater number of channels.

In [52] frequency diversity has been used in response to low key extraction efficiency of static and slow moving wireless environments. The scheme consists in a continuous changing of the frequency during the channel probing phase, a technique referred to as frequency hopping, to capture the channel frequency response and increase the available randomness. Moreover, channel estimates are initially filtered to remove sharp changes of amplitude due to noises and subsequently converted into a standard double-threshold quantisation. Investigated pre-processing methods include a moving average and a more sophisticated principal component analysis (PCA) based on the diagonalisation of the co-variance matrix. During the tests, the protocol achieves a near zero disagreement rate and a higher key generation efficiency compared to work in [23], which emphasises the superior ability of transforming raw-data in key bits. Nonetheless, the empirical process used to identify the system parameters considered only three frequency steps without taking into account the relationship with the dynamic characteristics of the channel.

The contribution of principal component analysis is also investigated in [53] where theory and Monte Carlo simulations agreed on considering PCA a better pre-processing method than discrete cosine transform (DCT) and wavelet transform (WT), regarding its ability to achieve a higher generation rate. Authors also extended their previous work [50] by contrasting two versions of PCA based on private and common eigenvectors. The need to publicly transmit eigenvalues stems from the consideration that even small discrepancies between the legitimate nodes result in significantly different eigenvectors which in turns, lead to an uncorrelated reconstruction of the signal. Moreover, the process of eigenvalue decomposition is computationally expensive and it could be advantageous to have only one side to perform these calculations. Even considering the number of bits wiped out during the privacy amplification step to balance the information leakage, PCA with common eigenvector gives better results than its private version. However, its complexity requires at least one side with relevant computational capabilities, hence it does not seem to be appropriated in low-end sensor networks.

An interesting property of orthogonal frequency-division multiplexing (OFDM) systems is their ability to minimise frequencies' interference by construction, where the signal is divided in parallel streams which are independently modulated in separated sub-carriers. The latter can be thought of as a set of narrowband channels usable as multiple sources of randomness, therefore, further increasing the key generation rate. This approach has been explored in [49] where the hardware and electrical differences generated, greatly influence the channel state information rendering it

significantly non-reciprocal even in the same coherence time interval. To address this unexpected obstacle, a new algorithm, called Channel Gain Complement (CGC), mitigates such a discrepancy after an initial learning phase. Empirical tests showed how CSI non-reciprocity depends on both noise, which is statistically independent and identically distributed, as well as a more stable component associated to each sub-carrier.

According to this consideration, after a small number of initial probes noise influence becomes less and less critical, permitting the estimate of the stable component to be later removed to achieve a lower bit mismatch. A multi-level quantisation step is executed in the domain frequency which separately quantises each amplitude associated to a different sub-carrier of the OFDM system. Furthermore, quantisation levels are dynamic and chosen depending on the variance of the reciprocity differentials acquired during the learning phase. The scheme seems to suffer in indoor environments where the high dynamic multipath phenomena induce a sharp increase in error probability. On the other hand, channel impulse responses have proven to be resilient to channel predictability attacks, because the sub-carriers CIR trends are very different, i.e. not being correlated to the specific line-of-sight situation as in any RSS-based approaches.

### *3.3. CIR based methods*

RSSI is an essential characteristic of the channel, widely available which fails to explore the channel diversity and multipath behaviour. On the other hand, channel impulse response (CIR) gives more detailed information about the channel state through a collection of distinct multipath components, which compose a train of discrete pulses with different magnitudes and delays, individually modelled through Rician or Rayleigh fading. This finer-grained description of the channel can further be converted into secret key bits. In [54] key extraction from jointly Gaussian random variables was investigated, dragged by the fact that wireless channel taps possess a complex Gaussian distribution [80]. The secret key capacity was defined as a function of SNR and simulations were performed on two distinct quantisation schemes, based on equally likely levels and a minimum mean square error technique (MMSE). Results showed that even if the MMSE quantisation leads to a lower BER, its output requires an entropy compensation algorithm which at the end, generates as many bits as the equiprobable quantisation scheme. In contrast, the evaluation of both Gray and natural codes in an LDPC-driven error reconciliation confirms the significantly higher performance of the former.

An extension of the previous protocol was successfully applied in International Telecommunication Union (ITU) cellular channels [55]. Instead of taking only one sample per CIR observation, scientists improved the protocol to sample each path. The main challenge was to remove the statistical dependence among Alice and Bob's CIR samples while keeping the high correlation with the other communicating party. Independent samples cannot be obtained by standard compression techniques as they amplify the small differences at their input, producing bit-streams that hardly match. However, an orthogonal greedy algorithm (OGA) has been introduced to repetitively decompose the channel in taps, converted through quantisation and error correcting codes as in the original scheme [54]. Despite the lack of practical tests, the simulations pointed out that the extension shares the same performance curve as in the inspiring method.

In the previous scheme, nodes' mobility is the primary source of randomness, however, this role can also be occupied by location-based information. In [56], both parties extract the shared key by applying a previously agreed function on CIR measurements acquired at previous locations. The function is used to increase the secret space, as in the case of permuting individual measurements, quantised in a novelty scheme, called Jigsaw Encoding, to overcome the inability of uniform quantisation to keep a low BMR while increasing the number of the levels. In fact, uniform quantisation is unable to emphasise how close the corresponding outputs have been, while due to high correlation, in a PLS protocol a mismatch usually involves two consecutive bins. Using two matrices of random numbers, Jigsaw Encoding translates quantisation outputs into vectors of numbers which differ in few slots quickly recovered by a polynomial correcting code, providing a bit generation of 3-5 bits for each estimate and sufficient entropy. The security of the algorithm is based on the assumption that only Alice and Bob are capable of getting accurate and correlated estimates and that the adversary does not exactly know all the positions involved in the key generation phase, especially when the number of considered locations is sufficiently large. An interesting observation is that location-based CIR uniqueness and channel variations due to movements could be used on a mutual basis to strengthen existing algorithms.

Similarly to RSS-based approaches, CIR-based techniques benefit from their application in MIMO systems. In [108], the theoretical limits of secret key extraction in MIMO systems have been established, followed by a pilot experiment in [57] that confirmed the possibility of achieving a high key generation rate (about 60 bits/estimate for a four-antenna array). Two practical quantisation algorithms have been proposed as a better replacement of direct channel quantisation. The first

one, called Channel Quantisation with Guardband (CQG), is a generalisation of the standard censor protocol [22] where both amplitude and phase are quantised in equally probable guard-banded levels which are iteratively constructed as in [109]. In the second technique, referred to as Channel Quantisation Alternating (CQA), guard-bands are replaced with two alternative quantisation maps that suggest to Bob which side of the complex channel sectors he should consider. Monte Carlo simulations showed that CQA performs better with the increase of the number of quantisation levels where CQG struggles to maintain a low BMR.

Mathematical expressions of BER and key generations efficiency of CQG were defined in [110], where an information reconciliation step built on Slepian-Wolf lossless compression coding was also introduced. Simulations proved that maximum efficiency could be achieved by an adequate choice of guard band regions and LDPC codes. Such parameters were later formally derived in [47]. Nevertheless, authors claimed that the use of guard interval is a suboptimal solution regarding key generation rate because of the drop of channel taps whose phases lay under an invalid region. In their successive work [58] they introduced an intelligent algorithm based on phase shifting toward some constellation points without any loss of secrecy, to transform the reconciliation problem into a normal demodulation task. The proposed algorithm can extract 120 secret bits from a single channel observation, however, it is based on impractical assumptions on channel estimation, as well as reciprocity, further analysed in [59]. In [59], an efficient 3-way extraction procedure was introduced to make the scheme less susceptible to channel variations. Furthermore, the role of mobility was investigated and simulations confirmed that it is in fact an advantage, as it allows a faster temporal decorrelation of the channel and a faster key refresh. A precise formalisation of the advantageous role of mobility remains to be researched.

The vast majority of cases relies on scalar quantisation where each channel estimate is separately converted. In [63] authors claim that vector quantisation is needed to fully exploit the correlation among channel samples and to efficiently resolve the cell-boundary problem which coincides with the high probability of disagreement of estimates falling close to quantisation bins' boundaries. The proposed scheme arises from the generalisation of CQG and CQA approaches, in which Alice and Bob choose a quantisation variant in order to minimise the BMR. Furthermore, instead of generating a number of different variants, which would require significant computational complexity and memory footprint, the scheme introduce a rotation-base vector quantiser where rotation matrices move channel vectors away from boundaries. The main drawback of vector quantisation is its strong

connection with the level of uncertainty from the adversary point of view: if Eve's observations are correlated to the ones of Alice or Bob, the key will be more easily guessed. For this reason the scheme also proposes the use of clustered key mapping which consists in an increased number of quantisation cells that enhances the overall robustness at the expense of worse BMR.

In reference [60] BGR is increased by generating bits from sub-carriers' CIRs, modelled as wide sense stationary uncorrelated scattering random processes. Quantisation is based on the cumulative distribution function to approximately have the same amount of 0s and 1s, extracted from subcarriers' channel impulse responses. In their work [61, 62], authors improved the scheme by designing a low pass filter which aims to reduce the effects of noise and, moreover, they introduced a rigorous modelling and analysis of the auto-correlation functions in both time and frequency domains. In contrast to other schemes in the literature, the filter is not empirically determined but arises from a mathematical modelling of channel reciprocity, resulting in a reduction of the disagreement rate in all simulations.

### *3.4. Miscellaneous approaches*

Besides the previously proposed channel characteristics, there some schemes which explore the domain from a different perspective and exploit different properties of the wireless medium. In [16] the fluctuation of BER is considered a promising source of randomness since it embraces all variabilities related to amplitude, phase, multipath delays, etc. Furthermore, a protocol is proposed to calculate BER in a hypothetical OFDM system as the average value of all sub-carriers and then quantise it using the median value as the threshold. Unfortunately, the key agreement rate is susceptible to low SNR and high fading frequencies. Moreover, existing low BERs (less than $10^{-3}$) represent insufficient sources of randomness and hence need to be amplified with artificial distortions, a fact that limits further the protocol's possible application scenarios.

Most of the work in physical layer security is about the transmission of data and its additional non-reciprocity compensation. On the contrary, in [17] researchers introduced a reverse pilot protocol in which the receiver transmits pilot signals so as the transmitter can use the channel estimation to compensate and encode the transmission, thus obtaining an automatic symbol level encryption at the channel level very similar to a shift decipher. The security of this protocol is based on the assumption that an attacker has no ways to correctly estimate the channel because the transmitter does not send any reference signals. However, the feasibility and the strength of this study should

be further researched.

Similarly, in [66] scientists aim to manipulate the OFDM pilot tones to lower the quality of eavesdropper's estimates without the introduction of any artificial noise. In the first stage, the receiver broadcasts pilot symbols to the transmitter that has an equal chance to either manipulate them or not. Phases' manipulations are done according to a zero threshold which follows from their uniform distribution, whereas amplitude's threshold is more complex and empirically set. Simulations show that both manipulations are indeed able to increase Eve's BER, however, manipulations also increase the legitimate parties' BER, especially when applying phases' manipulation.

The frequency-selective channels in OFDM systems has been indirectly used to enhance the signal space diversity (SSD), which consists in the separated transmission of quadrature components through independent fading channels. In [68], the interleaving pattern of the quadrature components is adaptively established in the frequency domain of sub-carriers, which usually demonstrate uncorrelated channel behaviours. Unfortunately, it is not clear how the obtained gain in secrecy capacity translates in a faster bit generation rate. In [71], the beam-forming abilities of an electronically steerable parasitic array radiator (ESPAR) antenna are used to create artificial randomness of channel measurements. In the proposed scheme, Alice and Bob generate arrays of estimates larger than the desired key length, as a tolerance needed to address bit disagreements. These additional values are then removed by both parties around the median value, which is used as the single threshold in the quantisation stage. Despite the initial waste of values, the single threshold permits the extraction of one bit for each estimate, achieving a high bit generation rate, followed by information reconciliation and privacy amplification steps based on Bose-Chaudhuri-Hocquenghem (BCH) codes and unidirectional hash functions, respectively. Performances have been evaluated in underwater environments where the beam-forming pre-processing has proved to strike a better balance with a sufficient key generation rate at a significantly lower bit mismatch rate than the competitors [73].

The previous protocol has been extended with the application of an RSS-interleaving technique which randomises and strengthens the keys, achieving a very high probability (99.9998%) of the success of exchanging 128 bit keys every two seconds. Furthermore, in [72], the rank of RSSI profiles is calculated by sorting the estimates, which are later quantised in a multi-level quantisation step with equi-probable bins. The main drawback in these approaches is the need of special antennas solely applicable to very specific and expensive scenarios.

Another beam-forming-based technique is introduced in [74] for securing multiple input single output (MISO) systems, where the knowledge of legitimate users' channel state information permits the annihilation of inter-user interferences. On the contrary, CSI of the passive eavesdropper is not available at the transmitter. The scheme generates a specific code-book starting from the feedback of a set of registered users, chosen by semi orthogonal selection in the attempt to exclude the ones with poor channel conditions. Besides the negative effects on the main channel capacity, simulations show that interferences may also be used to disrupt eavesdropper communication, acting as zero-powered artificial noise and thus increasing the secrecy capacity.

The use of artificial noise in MIMO systems is investigated in [69]. Authors state that a minimum secrecy capacity could be guarantee if number of transmitting antennas is higher than ones available to the adversary. Moreover, the presence of amplifying nodes is an alternative to a multi-antennas equipped transmitter. The major drawback consists in the loss of power sacrificed by the transmitter in its attempt to disrupt the eavesdropper channel capacity. Beam-forming techniques and artificial noise-based schemes are not mutually exclusive, hence they may be used together as in reference [70]. In the proposed protocol, the directional modulation is based on the recently developed random frequency diverse array (RFDA) which maximises SNR in the legitimate direction, by means of both angle and range. A lower bound of the ergodic secrecy capacity is used to determine the amount of transmitting power which should be destined to artificial noise, spread in all direction to limit the eavesdropper effectiveness.

Another power-expensive technique is introduced in [19] where a jamming technique, namely iJam, renders the scheme independent from channel variations, thus performing well even in static scenarios. The receiver jams copies of the transmitted message in a random and alternate fashion, preventing an eavesdropper to listen to the clean signal. However, the latter can be reconstructed by the receiver as he exactly knows which parts have been modified and where they are untouched. Tests showed that iJam is actually able to generate keys faster (3-18 kb/s) than conventional schemes with a negligible disagreement rate. This technique is built on previous studies on cooperative jamming [111] but it does not require an out-of-band channel to inform the receiver about the jamming signal.

Traditional half-duplex (HD) systems are not able to simultaneously sense the channel because the outgoing transmission generates a self-interference (SI) which is dominant in short distances, highly disturbing the perception of the desired signal. However, in recent times many suppression

techniques have been developed to minimise these phenomena leaving only some residuals (RSI) hence, allowing the growth of full-duplex (FD) wireless communication. In [75], full-duplex nodes simultaneously act as both receivers and jammers, to degrade the eavesdropper channel while receiving transmitted signals. Simulations confirmed that the proposed scheme achieves significant performance increments in contrast to the half-duplex case [19], with receivers equipped with both single and multiple antennas.

In [67], the authors evaluate the key generation capabilities of in-band full-duplex wireless devices (IBFD) by modelling those residuals as a zero mean Gaussian random variable whose variance is proportional to the emitted power. The study compares and contrasts the performance of both traditional and full-duplex systems showing that the latter permits a higher key rate especially when considering a low correlation coefficient where half-duplex approaches result in an unfeasible BER. Authors affirm that FD devices can sense highly volatile channel states, thus exploiting an additional amount of randomness which in turn, limits the key rate only to the performance of the SI-suppression circuitry.

## 4. Conclusion

The quantisation step is the core of the key generation process and its performance depends on both quantisation parameters (i.e. striking a balance between the number of thresholds and noise influence) as well as on the choice of the corresponding physical source of randomness. This survey aims to identify the most popular channel characteristics and corresponding quantisation schemes used to extract secret keys at the wireless physical layer in a comprehensive in depth state-of-play critical literature review of various approaches published to date. To evaluate the performance and robustness of each approach the fundamental and contrasting characteristics of BGR, BMR and Entropy were used as the key performance metrics throughout the discussion.

RSS based protocols could be easily implemented on current devices, requiring low hardware and computational complexity, which encourages their use in real-world scenarios. Nonetheless, a limitation of these protocols lies in the connection between the obtained entropy and the mobility of the nodes as well as the objects between them, exposing potential vulnerabilities against imminent and active attacks. On the other hand, phase-based approaches do not suffer this weakness because frequency-phase information is not related to distance and moreover achieve high entropy even by extracting estimates at a rate not constrained by the channel coherence time. Furthermore, phase

estimation is non-trivial since it requires some synchronisation which may not be real in concrete implementations between participants. To further boost the key generation rate, both the multipath and frequency diversities of the wireless medium are further explored through the channel impulse response CIR, responsible for extracting fine-grained information about the channel state. Similarly to phase-based protocols, CIR-based schemes are also resilient to possible adversary attacks because multipath trends are not correlated to line-of-sight (LOS) components, thus not easily predictable.

In the majority of the schemes, imperfect reciprocity is passively accepted and its errors are addressed in the information reconciliation step. Nonetheless, only a few preventive and compensation techniques have been applied to date, as in the interpolation with cubic Farrow filters [25, 31] or in techniques using low-pass filters [21, 49, 61, 112]. This aspect has not been sufficiently elaborated in the current research even if could potentially reduce the diminishing returns caused by information reconciliation.

The present review pinpoints and elicits that further work is required, which will build on existing theory and make full use of the increased amount of channel information in specific time-intervals and environmental conditions, while simultaneously shielding key entropy and robustness in contexts exhibiting a slowly degenerating changing state. In addition, to the best of our knowledge, the implications derived from the applications of the existing secret-key extraction schemes into specific real-life scenarios, as in the case of VANETs and WSNs, are insufficiently researched. These networks, however, possess particular challenging characteristics which could possibly induce either positive or negative effects that may in turn affect the performance of the extraction processes, especially during the distillation stage. Moreover, new and updated criteria and guidelines need to be introduced in the choice of optimal quantisation thresholds and global parameters, with a view to further improve existing and damaging trade-offs.

**References**

**References**

[1] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, Vol. 19964964 of Discrete Mathematics and Its Applications, CRC Press, 1996. arXiv:arXiv:1011.1669v3, doi:10.1201/9781439821916.

[2] R. Oppliger, Contemporary Cryptography, 2nd Edition, Artech House, Inc., Norwood, MA, USA, 2011.

[3] C. Boyd, A. Mathuria, Protocols for Authentication and Key Establishment, Information Security and Cryptography, Springer Berlin Heidelberg, Berlin, Heidelberg, 2003. doi:10.1007/978-3-662-09527-0.

[4] R. Y. Chang, S.-J. Lin, W.-H. Chung, Diffie-Hellman key distribution in wireless multi-way relay networks, in: 2013 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, IEEE, 2013, pp. 1–4. doi:10.1109/APSIPA.2013.6694207.

[5] P. Karadimas, Outdoor Channels, in: LTE-Advanced and Next Generation Wireless Networks, John Wiley & Sons, Ltd, Chichester, UK, 2012, pp. 97–122. doi:10.1002/9781118410998.ch4.

[6] G. Smith, A Direct Derivation of a Single-Antenna Reciprocity Relation for the Time Domain, IEEE Transactions on Antennas and Propagation 52 (6) (2004) 1568–1577. doi:10.1109/TAP.2004.830257.

[7] G. Durgin, Space-Time Wireless Channels, Space-Time Wireless Channels (2002) 1–19doi:10.1300/J155v04n04_01.
URL http://www.ncbi.nlm.nih.gov/pubmed/23834000

[8] A. D. Wyner, The Wire-Tap Channel, Bell System Technical Journal 54 (8) (1975) 1355–1387. doi:10.1002/j.1538-7305.1975.tb02040.x.

[9] C. H. Bennett, G. Brassard, J.-M. Robert, Privacy Amplification by Public Discussion, SIAM Journal on Computing 17 (2) (1988) 210–229. doi:10.1137/0217014.

[10] U. Maurer, Secret key agreement by public discussion from common information, IEEE Transactions on Information Theory 39 (3) (1993) 733–742. doi:10.1109/18.256484.

[11] J. Hershey, A. Hassan, R. Yarlagadda, Unconventional cryptographic keying variable management, IEEE Transactions on Communications 43 (1) (1995) 3–6. doi:10.1109/26.385951.

[12] Y. E. H. Shehadeh, D. Hogrefe, A survey on secret key generation mechanisms on the physical layer in wireless networks, Security and Communication Networks 8 (2) (2015) 332–341. arXiv:0806.0557, doi:10.1002/sec.973.
URL http://doi.wiley.com/10.1002/sec.973

[13] T. Wang, Y. Liu, A. V. Vasilakos, Survey on channel reciprocity based key establishment techniques for wireless systems, Wireless Networks 21 (6) (2015) 1835–1846. doi:10.1007/s11276-014-0841-8.

[14] Y. Zou, J. Zhu, X. Wang, L. Hanzo, A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends, Proceedings of the IEEE 104 (9) (2016) 1727–1765. arXiv:1505.07919, doi:10.1109/JPROC.2016.2558521.

[15] Y. Liu, H.-H. Chen, L. Wang, Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges, IEEE Communications Surveys & Tutorials XX (c) (2016) 1–1. doi:10.1109/COMST.2016.2598968.

[16] T. Kitano, A. Kitaura, H. Iwai, H. Sasaoka, A Private Key Agreement Scheme Based on Fluactions of BER in wireless Communications, in: The 9th International Conference on Advanced Communication Technology, Vol. 3, IEEE, 2007, pp. 1495–1499. doi:10.1109/ICACT.2007.358651.

[17] G. R. Tsouri, D. Wulich, Reverse piloting protocol for securing time varying wireless channels, in: 2008 Wireless Telecomunications Symposium, IEEE, 2008, pp. 125–131. doi:10.1109/WTS.2008.4547555.

[18] B. Zan, M. Gruteser, Random channel hopping schemes for key agreement in wireless networks, in: 2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications, IEEE, 2009, pp. 2886–2890. doi:10.1109/PIMRC.2009.5450011.

[19] S. Gollakota, D. Katabi, Physical layer wireless security made fast and channel independent, in: 2011 Proceedings IEEE INFOCOM, IEEE, 2011, pp. 1125–1133. doi:10.1109/INFCOM.2011.5934889.

[20] M. Tope, J. McEachen, Unconditionally secure communications over fading channels, in: 2001 MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force (Cat. No.01CH37277), Vol. 1, IEEE, 2001, pp. 54–58. doi:10.1109/MILCOM.2001.985763.

[21] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, B. Yener, Robust key generation from signal envelopes in wireless networks, in: Proceedings of the 14th ACM conference on Computer and communications security - CCS '07, ACM Press, New York, New York, USA, 2007, p. 401. doi:10.1145/1315245.1315295.

[22] S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, Radio-telepathy, in: Proceedings of the 14th ACM international conference on Mobile computing and networking - MobiCom '08, ACM Press, New York, New York, USA, 2008, p. 128. doi:10.1145/1409944.1409960.

[23] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, S. V. Krishnamurthy, On the effectiveness of secret key extraction from wireless signal strength in real environments, in: Proceedings of the 15th annual international conference on Mobile computing and networking - MobiCom '09, ACM Press, New York, New York, USA, 2009, p. 321. doi:10.1145/1614320.1614356.

[24] Chunxuan Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, N. B. Mandayam, Information-Theoretically Secret Key Generation for Fading Wireless Channels, IEEE Transactions on Information Forensics and Security 5 (2) (2010) 240–254. arXiv:0910.5027, doi:10.1109/TIFS.2010.2043187.

[25] N. Patwari, J. Croft, S. Jana, S. Kasera, High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements, IEEE Transactions on Mobile Computing 9 (1) (2010) 17–30. doi:10.1109/TMC.2009.88.

[26] A. Kitaura, H. Iwai, H. Sasaoka, A Scheme of Secret Key Agreement Based on Received Signal Strength Variation by Antenna Switching in Land Mobile Radio, in: The 9th International

Conference on Advanced Communication Technology, Vol. 3, IEEE, 2007, pp. 1763–1767. doi:10.1109/ICACT.2007.358712.

[27] S. T. Ali, V. Sivaraman, D. Ostry, Secret Key Generation Rate vs. Reconciliation Cost Using Wireless Channel Characteristics in Body Area Networks, in: 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, IEEE, 2010, pp. 644–650. doi:10.1109/EUC.2010.103.

[28] D. S. Karas, G. K. Karagiannidis, R. Schober, Neural network based PHY-layer key exchange for wireless communications, in: 2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications, IEEE, 2011, pp. 1233–1238. doi:10.1109/PIMRC.2011.6139697.

[29] J. Croft, N. Patwari, S. K. Kasera, Robust uncorrelated bit extraction methodologies for wireless sensors, in: Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks - IPSN '10, ACM Press, New York, New York, USA, 2010, p. 70. doi:10.1145/1791212.1791222.

[30] B. Zan, M. Gruteser, F. Hu, Improving robustness of key extraction from wireless channels with differential techniques, in: 2012 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2012, pp. 980–984. doi:10.1109/ICCNC.2012.6167572.

[31] Hongbo Liu, Jie Yang, Yan Wang, Yingying Chen, Collaborative secret key extraction leveraging Received Signal Strength in mobile wireless networks, in: 2012 Proceedings IEEE INFOCOM, IEEE, 2012, pp. 927–935. doi:10.1109/INFCOM.2012.6195843.

[32] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, S. V. Krishnamurthy, Secret Key Extraction from Wireless Signal Strength in Real Environments, IEEE Transactions on Mobile Computing 12 (5) (2013) 917–930. doi:10.1109/TMC.2012.63.

[33] F. Zhan, N. Yao, Z. Gao, H. Yu, Efficient key generation leveraging wireless channel reciprocity for MANETs, Journal of Network and Computer Applications 103 (2018) 18–28. doi:10.1016/j.jnca.2017.11.014.
URL https://ac.els-cdn.com/S1084804517303909/1-s2.0-S1084804517303909-main.pdf?{_}tid=f2330bb5-395e-4b67-80d3-624300d2d80c{&}acdnat=

1526239098{_}6f94c249bf4b7a99aa70fffe416121b4http://linkinghub.elsevier.com/retrieve/pii/S1084804517303909

[34] K. Zeng, D. Wu, A. Chan, P. Mohapatra, Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks, in: 2010 Proceedings IEEE INFOCOM, IEEE, 2010, pp. 1–9. doi:10.1109/INFCOM.2010.5462004.

[35] Z. Li, H. Wang, H. Fang, Group-Based Cooperation on Symmetric Key Generation for Wireless Body Area Networks, IEEE Internet of Things Journal 4 (6) (2017) 1955–1963. doi:10.1109/JIOT.2017.2761700.

[36] P. Xu, K. Cumanan, Z. Ding, X. Dai, K. K. Leung, Group Secret Key Generation in Wireless Networks: Algorithms and Rate Optimization, IEEE Transactions on Information Forensics and Security 11 (8) (2016) 1831–1846. doi:10.1109/TIFS.2016.2553643.

[37] R. Guillaume, S. Ludwig, A. Muller, A. Czylwik, Secret key generation from static channels with untrusted relays, in: 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2015, pp. 635–642. doi:10.1109/WiMOB.2015.7348022.

[38] G. Epiphaniou, P. Karadimas, D. K. B. Ismail, H. Al-Khateeb, A. Dehghantanha, K.-K. R. Choo, Non-Reciprocity Compensation Combined with Turbo Codes for Secret Key Generation in Vehicular Ad Hoc Social IoT Networks, IEEE Internet of Things Journal (2017) 1–1doi:10.1109/JIOT.2017.2764384.

[39] M. Yuliana, Wirawan, Suwadi, Performance evaluation of the key extraction schemes in wireless indoor environment, in: 2017 International Conference on Signals and Systems (ICSigSys), IEEE, 2017, pp. 138–144. doi:10.1109/ICSIGSYS.2017.7967029.

[40] A. A. Hassan, W. E. Stark, J. E. Hershey, S. Chennakeshu, Cryptographic Key Agreement for Mobile Radio, Digital Signal Processing 6 (4) (1996) 207–212. doi:10.1006/dspr.1996.0023.

[41] H. Koorapaty, A. Hassan, S. Chennakeshu, Secure information transmission for mobile radio, IEEE Communications Letters 4 (2) (2000) 52–55. doi:10.1109/4234.824754.

[42] A. Sayeed, A. Perrig, Secure wireless communications: Secret keys through multipath, in: 2008 IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE, 2008, pp. 3013–3016. doi:10.1109/ICASSP.2008.4518284.

[43] M. Wilhelm, I. Martinovic, J. B. Schmitt, On key agreement in wireless sensor networks based on radio transmission properties, in: 2009 5th IEEE Workshop on Secure Network Protocols, IEEE, 2009, pp. 37–42. doi:10.1109/NPSEC.2009.5342245.

[44] M. Wilhelm, I. Martinovic, J. B. Schmitt, Secret keys from entangled sensor motes, in: Proceedings of the third ACM conference on Wireless network security - WiSec '10, ACM Press, New York, New York, USA, 2010, p. 139. doi:10.1145/1741866.1741889.

[45] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, N. Mandayam, ProxiMate, in: Proceedings of the 9th international conference on Mobile systems, applications, and services - MobiSys '11, ACM Press, New York, New York, USA, 2011, p. 211. doi:10.1145/1999995.2000016.

[46] Q. Wang, H. Su, K. Ren, K. Kim, Fast and scalable secret key generation exploiting channel phase randomness in wireless networks, in: 2011 Proceedings IEEE INFOCOM, IEEE, 2011, pp. 1422–1430. doi:10.1109/INFCOM.2011.5934929.

[47] Y. El Hajj Shehadeh, D. Hogrefe, An Optimal Guard-Intervals Based Mechanism for Key Generation from Multipath Wireless Channels, in: 2011 4th IFIP International Conference on New Technologies, Mobility and Security, IEEE, 2011, pp. 1–5. doi:10.1109/NTMS.2011.5720584.

[48] L. Yao, S. T. Ali, V. Sivaraman, D. Ostry, Decorrelating secret bit extraction via channel hopping in body area networks, IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC (2012) 1454–1459doi:10.1109/PIMRC.2012.6362577.

[49] H. Liu, Y. Wang, J. Yang, Y. Chen, Fast and practical secret key extraction by exploiting channel response, in: 2013 Proceedings IEEE INFOCOM, IEEE, 2013, pp. 3048–3056. doi:10.1109/INFCOM.2013.6567117.

[50] G. Li, A. Hu, L. Peng, C. Sun, The Optimal Preprocessing Approach for Secret Key Generation from OFDM Channel Measurements, in: 2016 IEEE Globecom Workshops (GC Wkshps), IEEE, 2016, pp. 1–6. doi:10.1109/GLOCOMW.2016.7849063.

[51] S. Baksi, J. Snoap, D. C. Popescu, Secret Key Generation Using One-Bit Quantized Channel State Information, in: 2017 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, 2017, pp. 1–6. doi:10.1109/WCNC.2017.7925527.

[52] L. Hu, F. Zhang, A. Hu, Y. Jiang, G. Li, A key generation scheme for wireless physical layer based on frequency hopping, Procedia Computer Science 131 (2018) 1104–1112. doi:10.1016/j.procs.2018.04.273.

[53] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, D. Cao, High-Agreement Uncorrelated Secret Key Generation Based on Principal Component Analysis Preprocessing, IEEE Transactions on Communications 6778 (c) (2018) 1–13. doi:10.1109/TCOMM.2018.2814607.

[54] C. Ye, A. Reznik, Y. Shah, Extracting Secrecy from Jointly Gaussian Random Variables, in: 2006 IEEE International Symposium on Information Theory, IEEE, 2006, pp. 2593–2597. doi:10.1109/ISIT.2006.262101.

[55] C. Ye, A. Reznik, G. Sternburg, Y. Shah, On the Secrecy Capabilities of ITU Channels, in: 2007 IEEE 66th Vehicular Technology Conference, IEEE, 2007, pp. 2030–2034. doi:10.1109/VETECF.2007.426.

[56] J. Zhang, S. K. Kasera, N. Patwari, Mobility Assisted Secret Key Generation Using Wireless Link Signatures, in: 2010 Proceedings IEEE INFOCOM, IEEE, 2010, pp. 1–5. doi:10.1109/INFCOM.2010.5462231.

[57] J. W. Wallace, R. K. Sharma, Automatic Secret Keys From Reciprocal MIMO Wireless Channels: Measurement and Analysis, IEEE Transactions on Information Forensics and Security 5 (3) (2010) 381–392. doi:10.1109/TIFS.2010.2052253.

[58] Y. El Hajj Shehadeh, O. Alfandi, K. Tout, D. Hogrefe, Intelligent mechanisms for key generation from multipath wireless channels, in: 2011 Wireless Telecommunications Symposium (WTS), IEEE, 2011, pp. 1–6. doi:10.1109/WTS.2011.5960848.

[59] Y. El Hajj Shehadeh, O. Alfandi, D. Hogrefe, On improving the robustness of physical-layer key extraction mechanisms against delay and mobility, in: 2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, 2012, pp. 1028–1033. doi:10.1109/IWCMC.2012.6314347.

[60] J. Zhang, A. Marshall, R. Woods, T. Q. Duong, Secure key generation from OFDM subcarriers' channel responses, in: 2014 IEEE Globecom Workshops (GC Wkshps), IEEE, 2014, pp. 1302–1307. doi:10.1109/GLOCOMW.2014.7063613.

[61] J. Zhang, R. Woods, A. Marshall, T. Q. Duong, An effective key generation system using improved channel reciprocity, in: 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2015, pp. 1727–1731. doi:10.1109/ICASSP.2015.7178266.

[62] J. Zhang, A. Marshall, R. Woods, T. Q. Duong, Efficient Key Generation by Exploiting Randomness From Channel Responses of Individual OFDM Subcarriers, IEEE Transactions on Communications 64 (6) (2016) 2578–2588. doi:10.1109/TCOMM.2016.2552165.

[63] Y.-W. P. Hong, L.-M. Huang, H.-T. Li, Vector Quantization and Clustered Key Mapping for Channel-Based Secret Key Generation, IEEE Transactions on Information Forensics and Security 12 (5) (2017) 1170–1181. doi:10.1109/TIFS.2017.2656459.

[64] Y. Wei, K. Zeng, P. Mohapatra, Adaptive Wireless Channel Probing for Shared Key Generation Based on PID Controller, IEEE Transactions on Mobile Computing 12 (9) (2013) 1842–1852. doi:10.1109/TMC.2012.144.

[65] A. Badawy, T. Khattab, T. El-Fouly, A. Mohamed, D. Trinchero, C.-F. Chiasserini, Secret Key Generation Based on AoA Estimation for Low SNR Conditions, in: 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), IEEE, 2015, pp. 1–7. doi:10.1109/VTCSpring.2015.7146072.

[66] M. Soltani, T. Baykas, H. Arslan, Achieving secure communication through pilot manipulation, in: 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Vol. 2015-Decem, IEEE, 2015, pp. 527–531. doi:10.1109/PIMRC.2015.7343356.

[67] A. Sadeghi, M. Zorzi, F. Lahouti, Analysis of key generation rate from wireless channel in in-band full-duplex communications, in: 2016 IEEE International Conference on Communications Workshops (ICC), IEEE, 2016, pp. 104–109. arXiv:1605.09715, doi:10.1109/ICCW.2016.7503772.

[68] M. Yusuf, H. Arslan, On signal space diversity: An adaptive interleaver for enhancing physical layer security in frequency selective fading channels, Physical Communication 24 (2017) 154–160. doi:10.1016/j.phycom.2017.07.001.

[69] S. Goel, R. Negi, Guaranteeing Secrecy using Artificial Noise, IEEE Transactions on Wireless Communications 7 (6) (2008) 2180–2189. doi:10.1109/TWC.2008.060848.

[70] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, Y. Zhang, Artificial-Noise-Aided Secure Transmission With Directional Modulation Based on Random Frequency Diverse Arrays, IEEE Access 5 (2017) 1658–1667. doi:10.1109/ACCESS.2017.2653182.

[71] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, H. Sasaoka, Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels, IEEE Transactions on Antennas and Propagation 53 (11) (2005) 3776–3784. doi:10.1109/TAP.2005.858853.

[72] Shimpei Yasukawa, Hisato Iwai, Hideichi Sasaoka, A secret key agreement scheme with multi-level quantization and parity check using fluctuation of radio channel property, in: 2008 IEEE International Symposium on Information Theory, IEEE, 2008, pp. 732–736. doi:10.1109/ISIT.2008.4595083.

[73] Y. Luo, L. Pu, Z. Peng, Z. Shi, RSS-based secret key generation in underwater acoustic networks: advantages, challenges, and performance improvements, IEEE Communications Magazine 54 (2) (2016) 32–38. doi:10.1109/MCOM.2016.7402258.
URL http://ieeexplore.ieee.org/document/7402258/

[74] B. Özbek, Ö. Özdoğan Şenol, G. Karabulut Kurt, Secure multiuser MISO communication systems with limited feedback link, Annales des Telecommunications/Annals of Telecommunications (2018) 1–10doi:10.1007/s12243-018-0627-6.

[75] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, B. Ottersten, Improving Physical Layer Secrecy Using Full-Duplex Jamming Receivers, IEEE Transactions on Signal Processing 61 (20) (2013) 4962–4974. doi:10.1109/TSP.2013.2269049.

[76] C. E. Shannon, Communication Theory of Secrecy Systems*, Bell System Technical Journal 28 (4) (1949) 656–715. doi:10.1002/j.1538-7305.1949.tb00928.x.

[77] G. S. Vernam, Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications, Transactions of the American Institute of Electrical Engineers XLV (1926) 295–301. doi:10.1109/T-AIEE.1926.5061224.

[78] S. Leung-Yan-Cheong, M. Hellman, The Gaussian wire-tap channel, IEEE Transactions on Information Theory 24 (4) (1978) 451–456. doi:10.1109/TIT.1978.1055917.

[79] R. Ahlswede, I. Csiszar, Common randomness in information theory and cryptography. I. Secret sharing, IEEE Transactions on Information Theory 39 (4) (1993) 1121–1132. doi:10.1109/18.243431.

[80] A. Goldsmith, Wireless Communications, Vol. 9780521837, Cambridge University Press, Cambridge, 2005. arXiv:arXiv:1011.1669v3, doi:10.1017/CBO9780511841224.

[81] P. Karadimas, D. Matolak, Generic stochastic modeling of vehicle-to-vehicle wireless channels, Vehicular Communications 1 (4) (2014) 153–167. doi:10.1016/j.vehcom.2014.08.001. URL http://dx.doi.org/10.1016/j.vehcom.2014.08.001

[82] IEEE Computer Society, IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007) (2012) 1–2793doi:10.1109/IEEESTD.2012.6178212.

[83] G. Brassard, L. Salvail, Secret-Key Reconciliation by Public Discussion, in: Advances in Cryptology — EUROCRYPT '93, Springer Berlin Heidelberg, Berlin, Heidelberg, 1994, pp. 410–423. doi:10.1007/3-540-48285-7_35.

[84] J. D. Parsons, The Mobile Radio Propagation Channel, second edi Edition, John Wiley & Sons, Ltd, Chichester, UK, 2000. doi:10.1002/0470841524.

[85] Wei Xi, Xiang-Yang Li, Chen Qian, Jinsong Han, Shaojie Tang, Jizhong Zhao, Kun Zhao, KEEP: Fast secret key extraction protocol for D2D communication, in: 2014 IEEE 22nd International Symposium of Quality of Service (IWQoS), IEEE, 2014, pp. 350–359. doi:10.1109/IWQoS.2014.6914340.

[86] Chan Chen, M. A. Jensen, Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients, IEEE Transactions on Mobile Computing 10 (2) (2011) 205–215. doi:10.1109/TMC.2010.114.

[87] M. Zorgui, Z. Rezki, B. Alomair, E. A. Jorswieck, M.-S. Alouini, Secret-key agreement over spatially correlated multiple-antenna channels in the low-SNR regime, in: 2015 IEEE Conference on Communications and Network Security (CNS), IEEE, 2015, pp. 719–720. doi:10.1109/CNS.2015.7346902.

[88] B. T. Quist, M. A. Jensen, Maximizing the Secret Key Rate for Informed Radios under Different Channel Conditions, IEEE Transactions on Wireless Communications 12 (10) (2013) 5146–5153. doi:10.1109/TWC.2013.090313.122034.

[89] B. T. Quist, M. A. Jensen, Maximization of the Channel-Based Key Establishment Rate in MIMO Systems, IEEE Transactions on Wireless Communications 14 (10) (2015) 5565–5573. doi:10.1109/TWC.2015.2439684.

[90] E. A. Jorswieck, A. Wolf, S. Engelmann, Secret key generation from reciprocal spatially correlated MIMO channels, in: 2013 IEEE Globecom Workshops (GC Wkshps), IEEE, 2013, pp. 1245–1250. doi:10.1109/GLOCOMW.2013.6825164.

[91] Y. Liu, S. C. Draper, A. M. Sayeed, Exploiting Channel Diversity in Secret Key Generation From Multipath Fading Randomness, IEEE Transactions on Information Forensics and Security 7 (5) (2012) 1484–1497. arXiv:arXiv:1107.3534v2, doi:10.1109/TIFS.2012.2206385.

[92] A. Ambekar, H. D. Schotten, Enhancing Channel Reciprocity for Effective Key Management in Wireless Ad-Hoc Networks, in: 2014 IEEE 79th Vehicular Technology Conference (VTC Spring), Vol. 2015-Janua, IEEE, 2014, pp. 1–5. doi:10.1109/VTCSpring.2014.7022913.

[93] T. M. Cover, J. A. Thomas, Elements of Information Theory, Wiley-Interscience, New York, NY, USA, 1991.

[94] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, S. Vo, A statistical test suite for random and pseudorandom number generators for cryptographic applications,

Tech. Rep. April, National Institute of Standards and Technology, Gaithersburg, MD (2010). doi:10.6028/NIST.SP.800-22r1a.

[95] C. Cachin, U. M. Maurer, Linking information reconciliation and privacy amplification, Journal of Cryptology 10 (2) (1997) 97–110. doi:10.1007/s001459900023.

[96] T. Rappaport, Digital Communications: Fundamentals and Applications, 2nd Edition, Prentice Hall PTR, Upper Saddle River, NJ, USA, 2001.

[97] J. G. Proakis, Digital Communications, McGraw-Hill, 2001.

[98] R. Impagliazzo, L. A. Levin, M. Luby, Pseudo-random Generation from One-way Functions, in: Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing, STOC '89, ACM, New York, NY, USA, 1989, pp. 12–24. doi:10.1145/73007.73009.
URL http://doi.acm.org/10.1145/73007.73009

[99] P. Robyns, P. Quax, W. Lamotte, PHY-layer security is no alternative to cryptography, in: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks - WiSec '17, ACM Press, New York, New York, USA, 2017, pp. 160–162. doi:10.1145/3098243.3098271.

[100] N. Dottling, D. Lazich, J. Muller-Quade, A. S. De Almeida, Vulnerabilities of Wireless Key Exchange Based on Channel Reciprocity, in: Proceedings of the 11th International Conference on Information Security Applications, Springer-Verlag, Berlin, Heidelberg, 2011, pp. 206–220.

[101] S. Eberz, M. Strohmeier, M. Wilhelm, I. Martinovic, A Practical Man-In-The-Middle Attack on Signal-Based Key Generation Protocols, in: S. Foresti, M. Yung, F. Martinelli (Eds.), Computer Security – ESORICS 2012, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, pp. 235–252.

[102] M. Wilhelm, I. Martinovic, J. B. Schmitt, V. Lenders, Short paper: reactive jamming in wireless networks: how realistic is the threat?, in: Proceedings of the fourth ACM conference on Wireless network security - WiSec '11, ACM Press, New York, New York, USA, 2011, p. 47. doi:10.1145/1998412.1998422.

[103] M. Clark, Robust wireless channel based secret key extraction, in: MILCOM 2012 - 2012 IEEE Military Communications Conference, IEEE, 2012, pp. 1–6. doi:10.1109/MILCOM.2012.6415588.

[104] M. Bloch, J. Barros, M. R. D. Rodrigues, S. W. McLaughlin, Wireless Information-Theoretic Security, IEEE Transactions on Information Theory 54 (6) (2008) 2515–2534. arXiv:0611121, doi:10.1109/TIT.2008.921908.

[105] M. A. Forman, D. Young, A Generalized Scheme for the Creation of Shared Secret Keys through Uncorrelated Reciprocal Channels in Multiple Domains, in: 2009 Proceedings of 18th International Conference on Computer Communications and Networks, IEEE, 2009, pp. 1–8. doi:10.1109/ICCCN.2009.5235210.

[106] A. Badawy, T. Elfouly, T. Khattab, A. Mohamed, M. Guizani, Unleashing the secure potential of the wireless physical layer: Secret key generation methods, Physical Communication 19 (2016) 1–10. doi:10.1016/j.phycom.2015.11.005.

[107] F. Gray, Pulse Code Communication (1953).

[108] J. Wallace, C. Chen, M. Jensen, Key Generation Exploiting MIMO Channel Evolution: Algorithms and Theoretical Limits, EuCAP 2009 (2009) 1499–1503.

[109] J. Wallace, Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits, in: 2009 IEEE International Conference on Communications, IEEE, 2009, pp. 1–5. doi:10.1109/ICC.2009.5199440.

[110] X. Sun, W. Xu, M. Jiang, C. Zhao, Improved Generation Efficiency for Key Extracting from Wireless Channels, in: 2011 IEEE International Conference on Communications (ICC), IEEE, 2011, pp. 1–6. doi:10.1109/icc.2011.5962502.

[111] R. Negi, S. Goel, Secret communication using artificial noise, in: VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005., Vol. 3, IEEE, 2005, pp. 1906–1910. doi:10.1109/VETECF.2005.1558439.

[112] S. T. Ali, V. Sivaraman, D. Ostry, Eliminating Reconciliation Cost in Secret Key Generation for Body-Worn Health Monitoring Devices, IEEE Transactions on Mobile Computing 13 (12) (2014) 2763–2776. doi:10.1109/TMC.2013.71.

**Mirko Bottarelli** was born in 1980 in Milan, Italy. He received his Bachelor and Master's degrees in Computer Science from Università degli Studi di Milano Bicocca, Milan, Italy in 2004 and 2006, respectively. He is currently pursuing a PhD degree in the Faculty of Science and Engineering at the University of Wolverhampton, UK. His research interests are in the area of wireless communication, information theory and physical layer security.

**Dr Gregory Epiphaniou** Dr Gregory has worked as cyber security consultant and trainer for QA Ltd with high engagement with several industry partners in Information security domains. He delivered a broad range of technical and bespoke certifications including but not limited to CISSP, CISMP, CEH and BCS. He was holding a position as a senior lecturer in Cybersecurity at the University of Bedfordshire and since Jan 2018, Gregory is an Associate Professor in Cybersecurity and Commercial director of the WCRI at the University of Wolverhampton. He has taught in many Universities both nationally and internationally a variety of areas related to Cybersecurity with over 50 international publications in journals, conference proceedings and author in several book chapters. He holds several industry certifications around Information Security, and worked with several government agencies including the MoD in Cybersecurity related projects. He currently holds a subject matter expert panel position in the Chartered Institute for Securities and Investments and acts as a technical committee member for several scientific conferences in Information and network security.

**Dhouha Kbaier** joined the University of Bedfordshire as a Lecturer in Telecommunications and Network Engineering in March 2016. She received from Telecom Bretagne (Brest, France) both her PhD in 2011 with the highest honours and her Master of Engineering degree in 2008. She was specialised in Space Communications Systems in the French "Grande École" ISAE in Toulouse, heart of the European Aerospace Industry. Prior to working at the University of Bedfordshire, she worked for several years as a post-doctoral research follower first at Telecom Bretagne, then with Thales Airborne Systems and finally at IFREMER. Thanks to her multi-disciplinarily and her diverse research background, Dr Kbaier was awarded in February 2016 by two French lecturer qualifications in two different fields. She is Fellow of the Higher Education Academy and an Engineering Professors' Council (EPC) member. Her research was particularly awarded by several productivity bonuses and an IEEE best paper award. Her research interests include signal processing applied to telecommunications and oceanography, channel coding, digital communications and information theory, error correction in VANET environments, etc.

**Petros Karadimas** was born in Tripolis, Greece. He completed his Diploma (MEng) and PhD degrees in the Department of Electrical and Computer Engineering, University of Patras, Greece, in 2002 and 2008, respectively. In December 2009, he was appointed as a Research Fellow in the Centre for Wireless Network Design (CWIND) at the Department of Computer Science and Technology of University of Bedfordshire in UK. He was appointed as a Lecturer in Electronic Engineering in the same Department in October 2011, where he was promoted to Senior Lecturer in August 2015. In August 2016, he moved to the University of Glasgow, UK, as a Lecturer in Electrical and Electronic Engineering. His research interests include Wireless Channel Characterization and Modeling, Multiple Antenna Systems and Physical Layer Security. His research has been funded by major research councils and funding organizations including UK's EPSRC and CDE/DSTL.

**Haider Al-Khateeb** specialises in Cyber Security, Digital Forensics and Incident Response (DFIR). He holds a first-class BSc (Hons) in Computer Science and PhD in Cyber Security. He is a university lecturer, researcher, consultant, trainer and a Fellow of the Higher Education Academy (FHEA), UK. Haider has published numerous professional and peer-reviewed articles on topics including authentication methods, IoT forensics, cyberstalking, anonymity and steganography. He is a lecturer in the School of Computer Science and Technology and conducts research within the Institute for Research in Applicable Computing (IRAC), University of Bedfordshire.